Inconsistent Processes and Procedures Result in Many Victims of Identity Theft Not Receiving Identity Protection Personal Identification Numbers

March 23, 2017

Reference Number: 2017-40-026

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.

INCONSISTENT PROCESSES AND PROCEDURES RESULT IN MANY VICTIMS OF IDENTITY THEFT NOT RECEIVING IDENTITY PROTECTION PERSONAL IDENTIFICATION NUMBERS

Highlights

Final Report issued on March 23, 2017

Highlights of Reference Number: 2017-40-026 to the Internal Revenue Service Commissioner for the Wage and Investment Division.

IMPACT ON TAXPAYERS

To provide relief to identity theft victims, the IRS began issuing Identity Protection Personal Identification Numbers (IP PIN) to eligible taxpayers in Fiscal Year 2011. An IP PIN is a six-digit number assigned to taxpayers that allows their tax returns/refunds to be processed without delay and helps prevent the misuse of their Social Security Numbers (SSN) on fraudulent Federal income tax returns. In Processing Year 2016, the IRS issued approximately 2.7 million IP PINs to taxpayers for use in filing their tax returns.

WHY TIGTA DID THE AUDIT

This audit was initiated to assess IRS actions to improve and expand the IP PIN Program. This includes assessing IRS corrective actions to TIGTA's prior recommendations and the IRS's decision to not deactivate the online IP PIN application after security weaknesses were identified.

WHAT TIGTA FOUND

The IRS did not deactivate the online IP PIN application after a security breach was identified on May 17, 2015. Instead, risk mitigation processes were implemented. TIGTA made repeated recommendations to shut down the application until a stronger level of online authentication could be implemented and advised the IRS that its risk mitigation processes were not always working as intended.

TIGTA's review of 32,623 tax returns, filed between January 19 and May 24, 2016, with an IP PIN that was viewed online identified that 12,020 (36.8 percent) returns were not manually reviewed as required.

TIGTA also identified that taxpayer accounts were not always consistently updated to ensure that IP PINs were generated for taxpayers as required. The IRS did not generate an IP PIN for approximately 2 million taxpayers for whom the IRS resolved an identity theft case confirming the taxpayer was a victim. Additionally, the IP PIN notice continues to contain inaccurate information. The IRS mailed approximately 2.7 million IP PIN notices to taxpayers for Processing Year 2016 erroneously instructing them not to use their IP PIN if they are claimed as a dependent on a tax return.

The IRS's Opt-In Program was designed to focus on taxpayers in locations with the highest per capita rate of identity theft and offer them the opportunity to obtain an IP PIN before becoming a victim of tax-related identity theft. However, the IRS has not updated its identification of locations that may now have the highest per capita rate based on identity theft complaints. In addition, taxpayers in Opt-In Program locations may be unaware of the option to obtain an IP PIN.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the IRS ensure that: 1) an authentication risk assessment is completed and documented subsequent to all future system security breaches to an online application; 2) all functions have consistent procedures for adding identity theft markers that create an IP PIN; 3) accurate information is provided to taxpayers on IRS notices; 4) processes are developed to identify taxpayers in locations with the highest per capita rate of identity theft; and 5) an outreach strategy is developed to increase taxpayer awareness of the Opt-In Program.

The IRS agreed with four recommendations but did not agree that processes need developing to identify taxpayers in locations with the highest per capita rate of identity theft. TIGTA stated that this decision is contrary to the intent of the Opt-In Program, which is to focus on taxpayers in States and locations with the highest per capita rate of identity theft.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

March 23, 2017

MEMORANDUM FOR COMMISSIONER, WAGE AND INVESTMENT DIVISION

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Inconsistent Processes and Procedures Result in Many Victims of Identity Theft Not Receiving Identity Protection Personal Identification Numbers (Audit # 201640017)

This report presents the results of our review to assess the Internal Revenue Service's actions to improve and expand the Identity Protection Personal Identification Number Program. This audit was part of our Fiscal Year 2016 Annual Audit Plan and addresses the major management challenge of Providing Quality Taxpayer Service Operations.

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

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).

Table of Contents

Appendices

Abbreviations

CP	Computer Paragraph
CY	Calendar Year
E-File	Electronically File(d)
IP PIN	Identity Protection Personal Identification Number
IPSO	Identity Protection Strategy and Oversight Office
IRS	Internal Revenue Service
PY	Processing Year
SSN	Social Security Number
TIGTA	Treasury Inspector General for Tax Administration

Background

Tax-related identity theft continues to be one of the biggest challenges facing the Internal Revenue Service (IRS). To provide relief to identity theft victims, the IRS began issuing Identity Protection Personal Identification Numbers (IP PIN) to eligible taxpayers in Fiscal Year[1] 2011. An IP PIN is a six-digit number assigned to taxpayers that allows their tax returns/refunds to be processed without delay and helps prevent the misuse of their Social Security Numbers (SSN) to file fraudulent Federal income tax returns. For Processing Year (PY)[2] 2016, the IRS issued more than 2.7 million IP PINs to taxpayers for use in filing their tax returns.

IP PINs are issued before each filing season,[3] and taxpayers who receive these numbers are instructed by the IRS to use them on their electronically filed (e-filed) and paper-filed tax returns to confirm their identity. The IRS will issue identity theft victims a new IP PIN each year for use in filing their tax return. The yellow highlighted section in Figure 1 provides an example of where primary filers should enter their IP PIN on Tax Year[4] 2015 Form 1040, *U.S. Individual Income Tax Return*, when filing a paper tax return.

Figure 1: Excerpt From Form 1040 With IP PIN Area Highlighted in Yellow

Sign Here	Under penalties of perjury, I declare that I have examined this return and accompanying schedules and statements, and to the best of my knowledge and belief, they are true, correct, and complete. Declaration of preparer (other than taxpayer) is based on all information of which preparer has any knowledge.			
Joint return? See instructions. Keep a copy for your records.	Your signature	Date	Your occupation	Daytime phone number
	Spouse's signature. If a joint return, **both** must sign.	Date	Spouse's occupation	If the IRS sent you an Identity Protection PIN, enter it here (see inst.)

Source: www.IRS.gov.

The IP PIN helps the IRS verify a taxpayer's identity and, as a result, accept his or her e-filed or paper-filed tax return. E-filed tax returns with an incorrect or missing IP PIN will be rejected until it is submitted with the correct IP PIN or the taxpayer files on paper. If the same conditions occur on a paper return, the IRS will delay processing the return and any refund due while it determines if the tax return was filed by the legitimate taxpayer.

[1] 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.
[2] The calendar year in which the tax return or document is processed by the IRS.
[3] The period from January through mid-April when most individual income tax returns are filed.
[4] A 12-month accounting period for keeping records on income and expenses used as the basis for calculating the annual taxes due. For most individual taxpayers, the tax year is synonymous with the calendar year.

The Identity Protection Strategy and Oversight Office (IPSO) is responsible for developing criteria to identify taxpayers who should receive an IP PIN

The IPSO, is located within the IRS's Wage and Investment Division Accounts Management function, and oversees the IP PIN process, including determining which taxpayers will be provided an IP PIN. For example, annually the IPSO provides the IRS Information Technology organization's Applications Development function with the criteria to identify taxpayers who will be issued an IP PIN.[5] The Applications Development function is responsible for developing the computer programming used to review tax accounts and identify taxpayers who meet IPSO criteria.

Assignment of an IP PIN

Each December, the IRS mails IP PINs to taxpayers who are confirmed by the IRS as victims of identity theft. These taxpayers previously received either an IRS letter or notice notifying them that an identity theft indicator was placed on their tax account. The identity theft indicator allows the IRS to track the types of identity theft incidents (IRS-identified or taxpayer-initiated) and the actions taken by employees on taxpayers' accounts.[6] The IRS sends Notice Computer Paragraph (CP) 01A, *We assigned you an Identity Protection Personal Identification Number*, which contains the IP PIN. Issuance of the notice and IP PIN is a systemic process based on identifying those tax accounts with certain identity theft indicators. Not all taxpayers whose tax accounts have an identity theft indicator will receive an IP PIN. For example, the IRS does not send an IP PIN to individuals who are deceased or for whom mail was previously returned undeliverable.[7]

The IRS also proactively offers an IP PIN to taxpayers who are at risk of potentially becoming an identity theft victim. For example, if a taxpayer calls the IRS to report a lost or stolen wallet or purse, the IRS will provide an IP PIN if the taxpayer successfully authenticates his or her identity. Successful authentication includes the taxpayer providing one or more valid Federal or State Government-issued forms of identification[8] and Form 14039, *Identity Theft Affidavit*, or a legible copy of a police report indicating identity theft. Another example is the initiative the IRS started in January 2014 whereby taxpayers who live in the District of Columbia, Florida, or Georgia can obtain an IP PIN online. These locations were selected because they had the highest per capita rate of tax-related identity theft when the initiative was piloted. The IRS established an IP PIN application on its public website (IRS.gov) to enable at-risk taxpayers the opportunity

[5] The Applications Development function is responsible for developing systems that manage taxpayer accounts from the initial filing of a tax return, interactions with taxpayers, and potential audit and collection activities.
[6] IRS-identified cases are those for which the IRS proactively identified the taxpayer as a potential identity theft victim. Taxpayer-initiated cases are those for which taxpayers initiated contact with the IRS; for example, to report that after filing a tax return they received a notice indicating that it was rejected because someone else (an identity thief) had already filed a tax return using the same SSN and name.
[7] If mail has been returned as undeliverable, this implies that the IRS does not have a good address for the taxpayer.
[8] Forms of identification include a Social Security card, passport, driver's license, or State identification card.

to obtain an IP PIN online.[9] These taxpayers must electronically authenticate their identity using the IRS's online authentication process before obtaining their IP PIN.

A prior Treasury Inspector General for Tax Administration (TIGTA) report cited that IP PINs were not provided to all eligible taxpayers

In September 2014,[10] we reported that the IRS did not provide an IP PIN to all taxpayers confirmed by the IRS as being a victim of tax-related identity theft. Specifically, we found 532,637 taxpayers who did not receive an IP PIN despite having an identity theft indicator on their tax account indicating that the IRS confirmed they were a victim of identity theft, resolved their case, and corrected their tax account. The IRS also had not provided an IP PIN to 24,628 taxpayers whose Personally Identifiable Information had been stolen, lost, breached, or disclosed by/from the IRS. In addition, we identified that the IP PIN notice issued to 759,446 taxpayers for PY 2013 did not provide adequate instructions on the use of the number and its importance on a tax return.

We recommended that the IRS: 1) ensure that IP PINs are consistently issued; 2) revise IP PIN issuance criteria to make eligible those taxpayers who have had their Personally Identifiable Information lost, breached, disclosed, or stolen and have authenticated themselves; and 3) revise the IP PIN notice to explain the effect on processing a recipient's tax return and refund when the number is not included on the filed tax return. The IRS agreed with the recommendations.

This review was performed with information obtained from the IPSO and Return Integrity and Compliance Services function in Washington, D.C.; Atlanta, Georgia; Holtsville, New York; and Austin, Texas, during the period October 2015 through October 2016. 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.

[9] The IRS refers to obtaining an IP PIN online as the opt-in process.
[10] TIGTA, Ref. No. 2014-40-086, *Identity Protection Personal Identification Numbers Are Not Provided to All Eligible Taxpayers* (Sept. 2014).

Results of Review

Actions Were Not Taken to Deactivate the Online Identity Protection Personal Identification Number Application Once a Security Breach Was Identified

In November 2015, we reported[11] that the IRS did not complete an authentication risk assessment of the IP PIN application when the application was first brought online. While IRS management recognized the IP PIN application required the use of multifactor authentication,[12] they believed that requiring multifactor authentication would further burden identity theft victims attempting to obtain an IP PIN. As a result, the IRS implemented its online IP PIN application using a single-factor authentication[13] process that was available in the IRS's authentication framework in Calendar Year (CY) 2015.

In this review, we identified that the IRS did not complete a sufficient risk assessment for the IP PIN application after discovering, on May 17, 2015, that the IRS single-factor authentication process had been breached by unauthorized individuals. The National Institute of Standards and Technology requires organizations, including the IRS, to complete an authentication risk assessment after it identifies a system security breach to mitigate the risks of known security vulnerabilities. The authentication risk assessment should be documented and include identified weaknesses, risks arising from the weaknesses, mitigation actions considered, and costs and resources required for the mitigation actions. Had the IRS conducted this required risk assessment, it may have concluded that the risk to victims and the IRS of having their IP PINs compromised warranted taking the application offline until authentication processes and procedures could be strengthened.

During the course of our review we repeatedly warned the IRS of the potential breaches to the IP PIN application. Despite these repeated warnings, the IRS allowed the application to remain active. For example, on January 8, 2016, we sent an e-mail alert to management recommending that the IRS not bring the IP PIN application back online (the application was taken offline on November 21, 2015, for system maintenance) until a stronger level of online authentication could be implemented. In response, IRS management noted that they shared our concerns and

[11] TIGTA Ref. No. 2016-40-007, *Improved Tax Return Filing and Tax Account Access Authentication Processes and Procedures Are Needed* (November 2015).
[12] Multifactor authentication is a characteristic of an authentication system or a token that uses two or more authentication factors to achieve authentication. The three types of authentication factors are something you know, something you have, and something you are.
[13] Single-factor authentication is a characteristic of an authentication system or a token that uses one of the three authentication factors to achieve authentication – something you know, something you have, or something you are.

developed mitigation strategies to address potential vulnerabilities when they brought the application back online on January 19, 2016.

The IRS implemented procedures in an attempt to mitigate IP PIN authentication risks

In response to concerns regarding IP PIN authentication, the IRS created processes to mitigate the risk of fraudulent tax returns being filed with IP PINs obtained from the IP PIN application for the 2016 Filing Season. The processes were intended to identify IP PINs obtained and scrutinize tax returns filed using these IP PINs. This strategy included the following processes:

- For tax returns with IP PINs that were revealed subsequent to January 18, 2016 (referred to as viewed), through the IP PIN application, the IRS planned to manually generate a list of individuals whose IP PIN was viewed and identify tax returns filed using one of these IP PINs to have IRS tax examiners manually review the returns unless the returns were already selected for review by another IRS process.
- For tax returns that included an IP PIN that was created using the online IP PIN application subsequent to January 18, 2016 (referred to as the opt-in process), the IRS planned to mark the tax accounts of individuals associated with these IP PINs to identify the returns and subject the returns to additional review using identity theft filters.[14]
- For tax accounts that were breached in the Get Transcript breach, a lock was placed on each victim's tax account to prevent the SSNs of confirmed and potential victims of the Get Transcript[15] breach from being used to access the IP PIN application.

During the 2016 Filing Season, before the IRS deactivated the IP PIN application on March 7, 2016, a total of 137,967 individuals revealed their IP PIN and 26,559 individuals opted-in for an IP PIN.

Some risk mitigation processes for the IP PIN application did not protect taxpayers

Our evaluation of the IRS's risk mitigation processes for the IP PIN application identified that these processes were not always effective in protecting identity theft victims from further use of their identities to file fraudulent tax returns. Specific mitigation processes not working as intended included:

[14] The identity theft filters incorporate criteria based on characteristics of confirmed identity theft tax returns to identify potentially fraudulent tax returns. These characteristics include amounts claimed for income and withholding, filing requirements, prisoner status, taxpayer age, and filing history.
[15] The Get Transcript Application allows taxpayers to view and download their tax information, such as account transactions, line-by-line tax return information, and income reported to the IRS.

- ***Required manual reviews to mitigate risk associated with IP PIN application accesses to view an IP PIN were not always performed as required.*** Our review of 32,623 tax returns filed between January 19 and May 24, 2016, with an IP PIN that was viewed online identified that 12,020 (36.8 percent) returns were not manually reviewed by a tax examiner as required. The IRS did not include the associated SSNs on its list of returns to be manually reviewed. IRS management was not certain of the reason in all cases, but management did state that some of these tax returns were not manually reviewed because system programming was not completed at the beginning of the 2016 Filing Season and because the IRS had insufficient staffing during the weekends to review tax returns received during the weekends. The IRS paid more than $42.4 million in refunds that were claimed on these 12,020 tax returns.

  Internal guidelines required the Returns Integrity and Compliance Services function to daily obtain a list of the SSNs associated with individuals whose IP PIN was viewed on the IP PIN application from the IRS's Information Technology organization. The list was to then be used to identify for review tax returns filed with these SSNs to determine whether the returns were suspicious.

- ***Processes to prevent online account access for the victims of the Get Transcript breach were not working as intended.*** Our review found 2,347 SSNs (of those identified by the IRS as potentially accessed by unauthorized individuals in the Get Transcript breach) that were used to either opt-in or reveal an IP PIN using the IP PIN application. Further analysis found that for 299 (12.7 percent) of the 2,347 SSNs, the IRS received a duplicate return with the SSN, which indicates a fraudulent tax return was likely filed by an identity thief who obtained the IP PIN from the IP PIN application. We notified the IRS of this issue on April 6, 2016.

On February 24, 2016, we again recommended that the IRS deactivate the online IP PIN application. Although the IRS implemented risk mitigation processes in a short amount of time and improved its processes as gaps and issues were identified, it did not deactivate the IP PIN application until March 7, 2016. To quantify the potential effect of the IRS not immediately deactivating the IP PIN application, we analyzed Tax Year 2015 filed tax returns with an IP PIN obtained from the online application. Our review identified that 23,991 (24 percent) of the 100,463 tax returns with refunds claimed totaling $26 million are potentially fraudulent. For each of these tax returns, the IRS did not receive a Form W-2, *Wage and Tax Statement*, supporting the income and withholding reported on the tax return.

While the lack of wage information from an employer is not necessarily a sign of identity theft, it is an indicator of a potentially fraudulent tax return. The IRS's processes require its employees to review Form W-2 information for a taxpayer as one of the steps to determine whether a tax return is fraudulent. Further analysis of the SSNs on the refund returns found that 11,749 (49 percent) taxpayers' accounts have an indicator that more than one return was filed using the

SSN. This duplicate filing indicator provides further evidence that the IRS may have processed an identity thief's fraudulent tax return with an IP PIN.

The IRS brought the IP PIN application back online on July 19, 2016, with improved security including multifactor authentication.

Recommendation

Recommendation 1: The Commissioner, Wage and Investment Division, should ensure that authentication risk assessments are completed and documented subsequent to all future identified system security breaches to an online application. This should include identification of weaknesses, risks arising from the weaknesses, mitigation actions to be considered, and costs and resources required for the mitigation actions.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS updated the incident response procedures on January 20, 2017, to require validation of the e-Authentication risk assessment. The validation will ensure that the risk assessment reflects the most recent known circumstances surrounding any future security-related incidents affecting online applications. Further, completion of the risk assessment validation and lessons learned will be documented in the incident notes.

Tax Accounts Were Not Always Consistently Updated to Ensure That Identity Protection Personal Identification Numbers Were Generated As Required

Our review identified approximately 2 million taxpayers for whom the IRS resolved an identity theft case as of December 29, 2015, but did not place a case resolution marker on their tax account that is used to generate an IP PIN. IRS officials stated that this results from inconsistent guidance among different functional areas as to case resolution in those instances in which the victims' address is unknown. For example, internal guidelines require employees in the Identity Theft Victim Assistance Directorate[16] to place a case resolution marker on the victim's tax account that will result in an IP PIN being created for the taxpayer even when the taxpayer's address is unknown. Conversely, internal guidelines notify employees in the Taxpayer Protection Program to *not place* an IP PIN-generating case resolution marker on the victim's tax account if the employee is unable to find an accurate taxpayer address.[17]

[16] This directorate is in the Accounts Management function. It was created to combine the skills of the Accounts Management function and the Small Business/Self-Employed Division's Compliance function in one organization to resolve identity theft cases and focus on the customer's experience.

[17] The Taxpayer Protection Program reviews tax returns that are proactively identified by the IRS as potential identity theft and stops fraudulent refunds before they are issued.

These inconsistent procedures will create burden for the 2 million taxpayers who do not have the marker on their account. For example, while these individuals do not have a marker that will result in the generation of an IP PIN, they do have an identity theft indicator as they are a confirmed victim of identity theft. As such, when they e-file subsequent tax returns, they will experience delays while the IRS manually reviews and processes their returns. If the IP PIN was created for the taxpayers, even if they do not receive it via a CP01A notice, a reject notification with helpful instructions on how to obtain their IP PIN will be provided to them when they attempt to e-file a subsequent tax return.

In addition, when the IRS does not create an IP PIN for taxpayers with resolved identity theft cases, it must use additional resources to review future tax returns received using the victims' SSNs. The following hypothetical example illustrates the inconsistent treatment:

> *Taxpayer A is a victim of tax-related identity theft and has his or her case resolved by the Identity Theft Victim Assistance Directorate. The employee who resolved the case did not know the taxpayer's address and, as detailed in internal guidelines, the employee lists the taxpayer address as an IRS campus[18] address. The employee places the required marker on the taxpayer's account that is used to generate an IP PIN for the taxpayer. In December, an IP PIN is generated for this taxpayer and, as such, will be required on all future tax returns filed with the taxpayer's SSN. When the taxpayer files his or her tax return, the taxpayer will receive a notification that he or she did not provide the required IP PIN on the return. The message directs the taxpayer to the IRS public website with directions on how to obtain his or her IP PIN. The taxpayer obtains an IP PIN and includes on it on his or her filed tax return which allows his or her tax returns/refunds to be processed without delay and helps prevent the misuse of his or her SSN to file fraudulent Federal income tax returns.*
>
> *Taxpayer B's IRS-initiated identity theft case is resolved by the Taxpayer Protection Program. The employee who resolves the case does not know the taxpayer's address and, as detailed in internal guidelines, the employee places an identity theft marker on Taxpayer B's account that does not result in an IP PIN being created for the taxpayer. As such an IP PIN is not required on future tax returns filed using Taxpayer B's SSN. When Taxpayer B files a tax return, the IRS will identify it as a filer with prior identity theft history and as such scrutinize his or her return, resulting in a delay in any refund due the taxpayer.*

When we brought this inconsistent taxpayer treatment to management's attention, they indicated that they were aware of the inconsistent processes to resolve IRS-identified identity theft cases. IPSO management agreed that the IRS processes should be updated to treat the cases consistently and indicated that they had started to evaluate their IP PIN processes in July 2016.

[18] The data processing arm of the IRS. The campuses process paper and electronic submissions, correct errors, and forward data to the Computing Centers for analysis and posting to taxpayer accounts.

Recommendation

Recommendation 2: The Commissioner, Wage and Investment Division, should ensure that all functions have consistent procedures for adding identity theft markers that create an IP PIN for all confirmed victims of identity theft whose current address cannot be confirmed.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS has the IP PIN Strategy working group reviewing functional processes and identifying inconsistencies with the procedural guidance associated with identity theft issues. The IRS is also in the process of developing a *Taxpayer Treatment Guide* as a corollary to the *Data Incident Response Guide*. The *Taxpayer Treatment Guide* will ensure a standard structure of incident response efforts relating to system and application security events. Through these two efforts, the IRS will establish a standard process for treating affected victims, whether they are self-identified, identified by the IRS through return processing activities, or subsequently identified as the result of a security incident.

The Identity Protection Personal Identification Number Notice Continues to Contain Inaccurate Information

Our review identified that the IRS mailed approximately 2.7 million CP01A notices for PY 2016 that erroneously instructed taxpayers not to use their IP PIN if they are claimed as a dependent on a tax return. These instructions conflict with PY 2016 e-file programming, which requires the IP PIN (even those assigned to a dependent) to be used on a filed tax return. Our review of Tax Year 2015 returns filed with an IP PIN found that 127,273 (9 percent) of 1.4 million rejected tax returns were rejected because of a missing dependent IP PIN. Many of these tax returns were likely rejected because the taxpayers followed the erroneous instructions in the CP01A notice they received.

In addition, the notice also erroneously stated that the IP PIN was to be used for Tax Year 2014 instead of Tax Year 2015. Inaccurate information in the CP01A notice is the same condition we reported in our September 2014 report. In our September 2014 report, we identified that the IP PIN notice did not provide taxpayers adequate instructions on how to use their IP PIN and the importance of using it on their tax return, and we recommended that the IRS revise the CP01A to include key information related to the use of an IP PIN for dependents, secondary filers, and taxpayers without a filing requirement.

On December 10, 2015, we notified the IRS of the inaccurate and confusing CP01A notice information about dependent IP PINs. In response, IRS management agreed that the language in the notice should be changed. However, the IRS was unable to update the language for PY 2016. They stated that they have not established a process to annually review high-impact and high-volume notices for accuracy when no revisions are made to the notice. Because the CP01A notice was not revised for PY 2016, it was not reviewed for accuracy. Management indicated

that they are working to develop a process to review high-impact and high-volume notices annually to ensure accuracy even if no revisions are made.

IRS management stated that they initiated the change request for the CP01A notice for a requested implementation date of January 2017. To address taxpayer confusion prior to that date, the IRS updated the *Understanding Your CP01A Notice* IP PIN section of its public website with language notifying the taxpayer of the IRS's error related to the incorrect year listed on the CP01A notice. Figure 2 shows the corrected language that the IRS posted on its website regarding the incorrect year on the CP01A notice.

Figure 2: Language in the "Understanding Your CP01A Notice" Section of the IRS Website Clarifying the Incorrect Year on the CP01A Notice

Due to an error, taxpayers are receiving Identity Protection PIN letters with an incorrect year listed. Taxpayers and tax professionals should be advised the IP PIN listed on the CP01A Notice dated January 4, 2016 is valid for use on all individual tax returns filed in 2016.

The notice incorrectly indicates the IP PIN issued is to be used for filing the 2014 tax return when the number is actually to be used for the 2015 tax return. The IRS emphasizes the IP PIN listed on the CP01A notice is valid for the 2015 returns. Taxpayers and their tax professionals should use this PIN number for 2015 tax returns, which the IRS will begin accepting from taxpayers starting Jan. 19, 2016.

The IRS apologizes for the confusion and any inconvenience.

Source: "Understanding Your CP01A Notice" section on the IRS website, as of May 14, 2016.

The IRS also updated its website to address the CP01A notice's inaccurate instructions regarding dependent IP PINs. However, our review of this corrected guidance found that the instructions are still insufficient because there is no mention of the inaccurate guidance in the CP01A notice nor advice to disregard the inaccurate guidance in the notice. Figure 3 provides the updated instructions on the website regarding the use of an IP PIN assigned to a dependent in CY 2016.

Figure 3: Instructions on the IRS Website Clarifying the Use of Dependent IP PINs for CY 2016

If you are filing a joint return using Form 1040, 1040A, 1040EZ or 1040 PR/SS

- **Electronic Returns**
  - Every taxpayer who receives an IP PIN must enter it on the return, this includes the primary taxpayer, spouse, and dependent.
    - If only one taxpayer receives an IP PIN, enter it with that taxpayer's SSN.
    - If both taxpayers receive an IP PIN, both taxpayers must enter the IP PIN with their SSN.
    - If your dependent has an IP PIN assigned prior to the filing season, you must include his or her IP PIN on your federal tax return.
- **Paper Returns**
  - Only the first taxpayer listed on the tax return must enter their IP PIN.

Note: The spouse's IP PIN still protects the joint account, even though it's not on the paper return.

Source: "Understanding Your CP01A Notice" section on the IRS website, as of May 14, 2016.

Recommendation

Recommendation 3: The Commissioner, Wage and Investment Division, should ensure that all information provided to taxpayers on the CP01A notice issued for PY 2017 is accurate.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS reviewed the PY 2017 CP01A notice for accuracy and sent it to approximately 3.5 million taxpayers in late December 2016.

Taxpayers in "Opt-In" Locations May Not Be Aware of the Option to Obtain an Identity Protection Personal Identification Number and These Locations Have Not Been Updated

The IRS did not sufficiently advertise the IP PIN Opt-In Program in PY 2014 and PY 2015 in an attempt to increase participation. For example, in PY 2014, the IRS marketed the program to only taxpayers residing in the District of Columbia, Florida, and Georgia who obtained an e-file PIN through the IRS's public website. These taxpayers received an invitation to opt-in for an IP PIN when their e-file PIN was displayed on the website. In PY 2015, the IRS used the Twitter social media site to advertise the IP PIN Opt-In Program. The IRS did not publish any information on Twitter advertising the IP PIN Opt-In Program in PY 2016. Figure 4 provides the IRS Twitter activity and number of outreach messages about IP PINs.

Figure 4: IRS Twitter Activity Related to IP PINs

Twitter Username	Number of Followers	Number of Information Messages	Number of IP PIN Information Messages
@IRSnews	70,158	10,091	7
@IRStaxpros	36,208	5,444	4
@YourVoiceAtIRS – Taxpayer Advocate	11,710	4,238	0
Total	**118,076**	**19,773**	**11**

Source: TIGTA review of IRS outreach using Twitter.

Our review identified that the Opt-In Program did not significantly increase the number of IP PINs obtained by taxpayers in the District of Columbia, Florida, and Georgia. As we previously discussed, the IRS started this initiative in PY 2014 that allowed taxpayers in these locations to obtain an IP PIN as part of its Opt-In Program. The IRS indicated that it used these three locations in its pilot because the Federal Trade Commission identified these locations as having the highest rate of identity theft per capita. Although the total number of individuals who have opted-in to obtain an IP PIN online increased from 10,635 in PY 2014 to 11,831 in PY 2016, the total number of individuals who have obtained an IP PIN is small when compared to the 13.4 million tax returns received from these three locations as of August 25, 2016. Figure 5 provides the total number of individuals residing in the three locations that opted-in for an IP PIN each year since the program started.

Figure 5: Opt-In Program Participation Rates for the District of Columbia, Florida, and Georgia for PY 2014 to PY 2016

Location	PY 2014	PY 2015	PY 2016	Total
District of Columbia	197	370	408	**975**
Florida	7,705	28,132	8,553	**44,390**
Georgia	2,733	7,095	2,870	**12,698**
Total	**10,635**	**35,597**	**11,831**	**58,063**

Source: The IPSO, as of August 25, 2016.

The IRS has not updated its identification of locations with the highest per capita rate of identity theft

The IRS's Opt-In Program was designed to focus on taxpayers in States and locations with the highest per capita rate of identity theft and offer them the opportunity to obtain an IP PIN before becoming a victim of tax-related identity theft. However, the IRS has not updated its identification of locations that may now have the highest per capita rate of identity theft based on

identity theft complaints. Figure 6 identifies the locations with the highest per capita rate of taxpayers with identity theft complaints for CYs 2013, 2014, and 2015.

Figure 6: Locations With the Highest Per Capita Rate of Identity Theft Complaints for CYs 2013 to 2015

Rank	CY 2013	CY 2014	CY 2015
1	Florida	Florida	Missouri
2	District of Columbia	Washington	District of Columbia
3	Georgia	District of Columbia	Connecticut

Source: The Federal Trade Commission's Consumer Sentinel Network Data Book for CYs 2013, 2014, and 2015.

IRS management was unaware that the locations with the highest per capita rate of identity theft had changed since the Opt-In Program started in January 2014. IRS management stated they are evaluating the entire IP PIN Program including the IP PIN Opt-In Program. They noted that they are not sure expanding the Opt-In Program to additional locations is the best alternative at this point. Management indicated that changing the States eligible for the program each year would strain the IRS's limited information technology resources, require additional communication to inform States that are no longer eligible and locations that became eligible, and confuse taxpayers as to whether they are eligible to receive an IP PIN. In addition, management indicated that the updated identity theft data for the prior year would not be available in time for the programming to be completed for the next filing season.

Management's position appears to be contrary to the intent of the Opt-In Program. The patterns of identity theft are constantly changing and, as such, processes and procedures also need to change. As Figure 6 shows the locations with the highest per capita rate of identity theft based on identity theft complaints has changed. Unfortunately, due to the lack of an updated analysis, the taxpayers in these locations who may be at a higher risk for becoming an identity theft victim than taxpayers in other locations are not proactively offered an IP PIN.

Recommendations

The Commissioner, Wage and Investment Division, should:

Recommendation 4: Develop processes and procedures to update and add to the Opt-In Program new locations that have the highest per capita rate of identity theft and offer taxpayers in these locations the opportunity to opt-in to the IP PIN Program and obtain an IP PIN online.

> ***Management's Response:*** The IRS disagreed with this recommendation. IRS management stated that given the costs and limitations of the IP PIN program, tracking identity theft demographics and implementing programs to change or increase the eligible population for the Opt-In Program would not be an effective use of limited resources.

The IRS believes that dedicating its limited resources to supporting and enhancing the multi-pronged protections and deterrents to identity theft refund fraud has paid significant dividends in helping protect taxpayers and reduce the victimization rate.

Office of Audit Comment: Taxpayers in Connecticut and Missouri faced the highest risk of identity theft in CY 2015 according to the Federal Trade Commission. The IRS's decision to not offer these taxpayers a chance to obtain an IP PIN through the Opt-In Program is contrary to the intent of the program, which is to focus on taxpayers in States and locations with the highest per capita rate of identity theft.

Recommendation 5: Develop an outreach strategy to increase taxpayer awareness in identified locations of the Opt-In Program.

Management's Response: The IRS agreed with this recommendation. The IRS will complete an analysis of the overall effectiveness of the IP PIN and Opt-In Programs. If it is determined that the Opt-In Program will continue, the IRS will develop an outreach strategy to increase taxpayer awareness of the Opt-In Program.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to assess IRS actions to improve and expand the IP PIN Program. To accomplish this objective, we:

I. Assessed the IRS's corrective actions to address TIGTA's prior recommendations related to the IP PIN Program.[1] We determined the effectiveness of the process the IRS established to ensure that IP PIN criteria are accurately programmed by the Applications Development function.

II. Assessed IRS plans for expanding and improving the IP PIN Program.

- A. Determined whether the IRS issued IP PINs to individuals who opt-in to receive an IP PIN.
- B. Evaluated the IRS's processes to ensure that dependents with IP PINs are adequately protected on the tax return. We reviewed the Notice CP01A to ensure that guidance was clear regarding the use of dependent IP PINs.

III. Assessed the IRS's business decision to not deactivate the IP PIN application when the Get Transcript breach was identified in May 2015.

IV. Evaluated the processes to identify potentially fraudulent tax returns filed with IP PINs obtained through the online IP PIN application.

- A. Evaluated the IRS's actions to mitigate the risk of fraudulent tax returns filed with an IP PIN that was viewed/revealed online.
- B. Identified the number of identity theft returns processed with an IP PIN obtained online, via opt-in or the reveal feature, and the number of taxpayers who experienced the burden of an identity thief filing a tax return with their IP PIN after stealing it from the IP PIN application in PY 2016.
- C. Determined the number of returns filed and the total amount of false refunds paid on returns with IP PINs that were revealed or opted-in through the IP PIN application.
- D. Matched the IRS's lists of IP PIN opt-in and revealed SSNs to the database of accepted e-file returns for PY 2016.

[1] TIGTA, Ref. No. 2014-40-086, *Identity Protection Personal Identification Numbers Are Not Provided to All Eligible Taxpayers* (Sept. 2014).

E. Determined how many taxpayer accounts have a Transaction Code 976 indicating a duplicate return was filed using the taxpayer's SSN. (A duplicate return indicates tax-related identity theft likely occurred.)

Validity and reliability of data from computer-based systems

Data used in this audit were validated by selecting independent samples of the IRS's list of IP PIN recipients received from the IRS to the taxpayer account information on the Individual Master File.[2] We validated the data in the Individual Returns Transaction Files,[3] the Modernized Tax Return Database,[4] and the Individual Master 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 System.[5] We determined that the data were valid and reliable for the purposes of this report.

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: decision criteria to not deactivate the IP PIN application after the Get Transcript breach was identified and to make it operational again without multifactor authentication; processes used to identify taxpayers authorized to receive an IP PIN; processes used to ensure the accuracy of the CP01A notices; and processes used to evaluate the performance of the IP PIN Opt-In Pilot Program. We evaluated these controls by interviewing personnel, reviewing IP PIN Program guidance and reports, and performing data analysis.

[2] The IRS database that maintains transactions or records of individual tax accounts.
[3] Contains data transcribed from initial input of the original individual tax returns during tax return processing.
[4] The legal repository for original e-filed returns received by the IRS through the Modernized e-File system.
[5] A large-scale computer system integrated with other IRS data systems and designed to provide instantaneous visual access to certain taxpayer accounts.

Appendix II

Major Contributors to This Report

Russell Martin, Assistant Inspector General for Audit (Returns Processing and Account Services)
Allen Gray, Director
Linna Hung, Audit Manager
Pamela DeSimone, Lead Auditor
Jerry Douglas, Lead Auditor
Laura Robertson, Auditor

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
Director, Accounts Management, Wage and Investment Division
Director, Office of Audit Coordination

Appendix IV

Outcome Measures

This appendix presents detailed information on the measurable impact that our recommended corrective 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; 2,028,042 taxpayers (see page 7).

Methodology Used to Measure the Reported Benefit:

The IRS continues to not provide IP PINs to all taxpayers identified as victims of identity theft. The IRS identifies taxpayers who are victims of identity theft and places markers on their tax accounts. However, inconsistent IRS procedures result in employees in some functions inputting markers that generate an IP PIN for the taxpayer, while employees in other functions input markers that do not generate an IP PIN. These inconsistent procedures may deprive 2,028,042 taxpayers, who did not have an IP PIN-generating identity theft marker placed on their account, of rights to which they are entitled. In addition, these taxpayers may experience additional burden related to their personal information being used by an identity thief.

Type and Value of Outcome Measure:

- Taxpayer Burden – Actual; 2,754,104 taxpayers (see page 9).

Methodology Used to Measure the Reported Benefit:

The IRS mailed approximately 2.7 million CP01A, *We assigned you an Identity Protection Personal Identification Number*, notices with inaccurate instructions for PY 2016. Our review of the CP01A notice found that it provides taxpayers with inaccurate instructions for dependent IP PIN use on a PY 2016 tax return. These instructions are not consistent with the IRS's PY 2016 e-file requirement for IP PIN use for all SSNs with an IP PIN. Specifically, it instructed taxpayers not to use the IP PIN if he or she was being claimed as a dependent on the tax return. In addition, the notice stated that the IP PIN contained in the CP01A notice was to be used for Tax Year 2014 instead of Tax Year 2015. The inaccurate instructions may create additional burden and delays for these taxpayers during the filing season. For example, our review of Tax Year 2015 tax returns as of May 3, 2016, found that 127,273 (9 percent) out of 1.4 million rejected tax returns were rejected because of an incorrect or missing dependent IP PIN.

Appendix V

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
ATLANTA, GA 30308

COMMISSIONER
WAGE AND INVESTMENT DIVISION

March 2, 2017

MEMORANDUM FOR MICHAEL E. MCKENNEY
DEPUTY INSPECTOR GENERAL FOR AUDIT

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

SUBJECT: Draft Audit Report – Inconsistent Processes and Procedures Result in Many Victims of Identity Theft Not Receiving Identity Protection Personal Identification Numbers (Audit # 201640017)

Thank you for the opportunity to review and provide comments on the subject draft report. The act of identity theft (IDT) refund fraud is a persistent threat to the tax system and its administration, constantly evolving and becoming more sophisticated as fraudsters attempt to defeat our protective controls. The IRS has made significant advances in our ability to protect taxpayers from the burdens associated with IDT refund fraud. Two such measures have been the development of the Identity Protection Personal Identification Number (IP PIN) program to assist known victims of IDT tax fraud, and the pilot testing of the Opt-In program, which is a proactive measure for protecting the accounts of individuals who have not yet been victimized by IDT fraud. Additionally, to improve the service and assistance provided to victims of IDT refund fraud, we consolidated our victim assistance operations under one directorate in July 2015.

The IRS began issuing IP PINs to eligible taxpayers in Fiscal Year 2011, to combat the growing threat of IDT refund fraud. The IP PIN is a six-digit number assigned to a taxpayer and must be used to file the tax return as a means of confirming the taxpayer's identity. To minimize the risk of IP PINs being compromised by fraudsters, new IP PINs are issued each year and mailed to the taxpayer's address. This process of an annual mailing of a new number to each IP PIN holder is not an ideal solution in that it creates certain burdens for taxpayers, and introduces administrative costs to the Government in printing and mailing the new number to eligible individuals. For one, it places responsibility on the taxpayer not to lose or misplace the number before its use when their tax return is filed. The loss of an IP PIN can cause electronically filed returns to be rejected and, if a paper return is filed, can delay the processing of that return and payment of any refund claimed while the IRS authenticates the identity of the person

filing the return. Further, once an IP PIN has been assigned to an account, that individual will continue to receive and be required to use that new number each year when filing their tax return. Obtaining a replacement IP PIN for one that was lost or misplaced can also impose additional delays on taxpayers' ability to file their returns and receive any refunds due. If taxpayers lose or misplace their IP PIN, they can access the IP PIN online tool, *Get An IP PIN*, and, after passing the newly implemented multifactor authentication process, retrieve their IP PIN. If they are unable to pass authentication, they must call the IRS or visit a walk-in location to authenticate and have their IP PIN mailed to them, which is likely to delay processing of their returns and refunds.

So, while the IP PIN has been an effective tool for protecting taxpayers from subsequent tax related IDT refund fraud, it is not a holistic or sustainable solution that can be applied to the more than 150 million returns that are filed annually each year. As such, the IRS continues to explore less burdensome and more nimble, adaptive and cost effective ways to verify the identity of filers at the time tax returns are submitted. We have taken other actions that have had a positive effect on the prevention of IDT refund fraud, as evidenced by increased numbers of potentially fraudulent returns being identified and stopped either at the time of filing or during return processing, as well as a commensurate 50 percent decrease in the volume of incoming claims of victimization. The IP PIN is only one tool in an increasingly sophisticated set of protections and deterrents to IDT refund fraud. These efforts include:

- working with external partners (e.g. tax preparation software industry, financial institutions, federal and state government agencies) through the Security Summit to identify additional opportunities to address IDT refund fraud;
- coordinating with external partners to develop and use new data elements to improve identification processes that result in better IDT refund fraud detection;
- piloting an Information Sharing and Analysis Center to test a robust exchange of information among state and industry participants for real-time response to fraud schemes, as well as advancing the capability to detect and prevent IDT refund fraud;
- using an active alert and rapid response process with our tax industry partners to elevate emerging tax administration issues and assist our partners in determining if similar threats are occurring within their own systems, thereby providing an early opportunity to address and mitigate threats of IDT refund fraud;

- establishing processes that identify and address potential IDT and non-compliant returns through systemic models, filters and business rules;
- improving the ability to identify IDT in a pre-refund environment, and improving processes to authenticate or validate third-party data and using it to assess potential fraud during return processing;
- implementing processes starting in the 2017 filing season that authenticate returns by taking advantage of the earlier receipt of wage and withholding information from employers, as provided by the earlier due date of Form W-2, *Wage and Tax Statement* required by the Protecting Americans from Tax Hikes Act of 2015; and
- expanding a new W-2 verification code authentication to verify the identity of the filer upon filing.

Prior to the March 7, 2016 deactivation of the IP PIN application on IRS.gov, an eAuthentication risk assessment (eRA) was performed in December 2015, while the application was offline for maintenance. In response to that risk assessment, which was performed under the standards of the Office of Management and Budget guidance OMB M-04-04, mitigating strategies were put into place when the application came online on January 19, 2016. These mitigation strategies were not as effective as had been expected and we made the decision to temporarily suspend access to the application. As noted in the report, the application was not made available again until July 19, 2016, after implementing a multifactor authentication process.

We have adopted the *Data Incident Response Playbook* for use in future emergency responses, based on the lessons learned from the Get Transcript incident. The playbook includes guidance for responding to incidents related to e-authentication and includes a requirement for validation of the eRA after any breach. The eRA validation will include observations and findings from lessons learned discussions in the detailed incident documentation.

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

Attachment

Attachment

Recommendation

The Commissioner, Wage and Investment Division, should:

RECOMMENDATION 1
Ensure authentication risk assessments are completed and documented subsequent to all future identified system security breaches to an online application. This should include identification of weaknesses, risks arising from the weaknesses, mitigation actions to be considered, and costs and resources required for the mitigation actions.

CORRECTIVE ACTION
We agree with this recommendation and updated our incident response procedures on January 20, 2017, to require validation of the e-Authentication risk assessment. The validation will ensure the risk assessment reflects the most recent known circumstances surrounding any future security-related incidents affecting online applications. Further, completion of the risk assessment validation and lessons learned will be documented in the incident notes.

IMPLEMENTATION DATE
Implemented

RESPONSIBLE OFFICIAL
Associate Chief Information Officer, Cybersecurity, Information Technology

CORRECTIVE ACTION MONITORING PLAN
N/A

RECOMMENDATION 2
Ensure that all functions have consistent procedures for adding identity theft markers that create an IP PIN for all confirmed victims of identity theft whose current address cannot be confirmed.

CORRECTIVE ACTION
We agree with this recommendation and have the Identity Protection Personal Identification Number (IP PIN) Strategy working group reviewing functional processes and identifying inconsistencies with the procedural guidance associated with identity theft (IDT) issues. We are also in the process of developing a Taxpayer Treatment Guide (TTG) as a corollary to the Data Incident Response Guide. The TTG will ensure a standard structure of incident response efforts relating to system and application security events. Through these two efforts, we will establish a standard process for treating affected victims, whether they are self-identified, identified by the IRS through return processing activities, or subsequently identified as the result of a security incident.

IMPLEMENTATION DATE
October 15, 2017

RESPONSIBLE OFFICIAL
Director, 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 3
Ensure that all information provided to taxpayers on the CP01A notice issued for PY 2017 is accurate.

CORRECTIVE ACTION
The 2017 Computer Paragraph 01A, *We assigned you an Identity Protection Personal Identification Number*, notice was reviewed for accuracy and sent to approximately 3.5 million taxpayers in late December 2016.

IMPLEMENTATION DATE
Implemented

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

CORRECTIVE ACTION MONITORING PLAN
N/A

Recommendations

The Commissioner, Wage and Investment Division, should:

RECOMMENDATION 4
Develop processes and procedures to update and add to the Opt-In Program new locations that have the highest per capita rate of identity theft and offer taxpayers in these locations the opportunity to opt-in to the IP PIN Program and obtain an IP PIN online.

CORRECTIVE ACTION
We disagree with this recommendation. Given the costs and limitations of the IP PIN program, tracking IDT demographics and implementing program changes to change or increase the eligible population for the Opt-In program would not be an effective use of limited resources. Dedicating our limited resources to supporting and enhancing the multi-pronged protections and deterrents to IDT refund fraud that we've established has

paid significant dividends in helping protect our taxpayers and reduce the victimization rate.

IMPLEMENTATION DATE
N/A

RESPONSIBLE OFFICIAL
N/A

CORRECTIVE ACTION MONITORING PLAN
N/A

RECOMMENDATION 5
Develop an outreach strategy to increase taxpayer awareness in identified locations of the Opt-In Program.

CORRECTIVE ACTION
We agree with this recommendation. Following the completion of our analysis of the overall effectiveness of the IP PIN and Opt-in programs, if it is determined that the Opt-in program will continue then we will develop an outreach strategy to increase taxpayer awareness of the program.

IMPLEMENTATION DATE
October 15, 2018

RESPONSIBLE OFFICIAL
Director, Accounts Management, Wage and Investment Division

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