



---

May 2016

# IDENTITY THEFT AND TAX FRAUD

## IRS Needs to Update Its Risk Assessment for the Taxpayer Protection Program

Accessible Version

# GAO Highlights

Highlights of [GAO-16-508](#), a report to congressional requesters

## Why GAO Did This Study

IRS estimates that, in 2014, it prevented or recovered \$22.5 billion in attempted IDT refund fraud, but paid \$3.1 billion in fraudulent IDT refunds. Because of the difficulties in knowing the amount of undetected fraud, the actual amount could differ from these point estimates. IDT refund fraud occurs when a refund-seeking fraudster obtains an individual's identifying information and uses it to file a fraudulent tax return. Despite IRS's efforts to identify and prevent IDT refund fraud, this crime is an evolving and costly problem.

GAO was asked to examine IRS's efforts to combat IDT refund fraud. This report (1) evaluates the performance of IRS's TPP and (2) assesses IRS's efforts to improve its estimates of IDT refund fraud costs for 2014. To evaluate TPP, GAO reviewed IRS studies, reviewed relevant guidance, and met with agency officials. Further, GAO conducted a scenario analysis to understand the effect of different assumptions on IRS's TPP analysis. To assess IRS's IDT cost estimates, GAO evaluated IRS's methodology against selected best practices in the *GAO Cost Guide*.

## What GAO Recommends

GAO recommends that IRS update its TPP risk assessment and take appropriate actions to mitigate risks identified in the assessment. GAO also recommends that IRS improve its IDT cost estimates by removing refund thresholds and using return-level data where available. IRS agreed with GAO's TPP recommendations and will update its risk assessment. IRS took action consistent with GAO's IDT cost estimate recommendations.

View [GAO-16-508](#). For more information, contact James R. McTigue, Jr. at (202) 512-9110 or [mctiguej@gao.gov](mailto:mctiguej@gao.gov)

May 2016

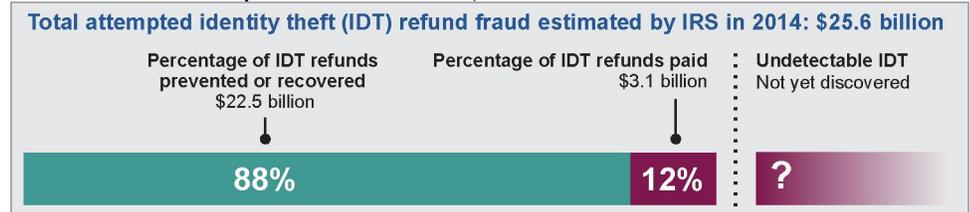
## IDENTITY THEFT AND TAX FRAUD

### IRS Needs to Update Its Risk Assessment for the Taxpayer Protection Program

## What GAO Found

**Taxpayer Protection Program (TPP).** While the Internal Revenue Service (IRS) has made efforts to strengthen TPP—a program to authenticate the identities of suspicious tax return filers and prevent identity theft (IDT) refund fraud—fraudsters are still able to pass through and obtain fraudulent refunds. TPP authenticates taxpayers by asking questions only a real taxpayer should know; however, fraudsters can pass by obtaining a taxpayer's personally identifiable information (PII). IRS estimates that of the 1.6 million returns selected for TPP, it potentially paid \$30 million to IDT fraudsters who filed about 7,200 returns that passed TPP authentication in the 2015 filing season; however, GAO's analysis suggests the amount paid was likely to be higher. Although IRS conducted a risk assessment for TPP in 2012, IRS has not conducted an updated risk assessment that reflects the current threat of IDT refund fraud—specifically, the threat that some fraudsters possess the PII needed to pass authentication questions. Federal e-authentication guidance requires agencies to assess risks to programs. An updated risk assessment would help IRS identify opportunities to strengthen TPP. Strengthened authentication would help IRS prevent revenue loss and reduce the number of legitimate taxpayers who become fraud victims.

#### IRS Estimates of Attempted IDT Refund Fraud, 2014



Source: GAO analysis of IRS data. | GAO-16-508

**IDT Refund Fraud Cost Estimates.** In response to past GAO recommendations, IRS adopted a new methodology in an effort to improve its 2014 IDT refund fraud cost estimates. However, the estimates do not include returns that fail to meet specific refund thresholds. IRS officials said the thresholds allow them to prioritize IRS's enforcement efforts. However, using thresholds could result in incomplete estimates. Improved estimates would help IRS better understand how fraud is evading agency defenses. The *GAO Cost Guide* states that cost estimates should include all relevant costs. Additionally, IRS's estimates of refunds it protected from fraud are based on the *Global Report*, which counts each time a fraudulent return is caught by IRS and thus counts some returns multiple times. IRS uses this data source because it is IRS's official record of IDT refund fraud. The *GAO Cost Guide* states that agencies should use primary data for estimates and the data should contain few mistakes. By using the *Global Report*, as opposed to return-level data, IRS produces inaccurate estimates of IDT refund fraud, which could impede IRS and congressional efforts to monitor and combat this evolving threat.

---

# Contents

---

---

Letter	1	
	Background	4
	Despite Recent Changes, Vulnerabilities in the Taxpayer Protection Program Limit IRS's Ability to Prevent IDT Refund Fraud	15
	IRS Improved Its Methodology for <i>Taxonomy</i> Estimates, but Has Not Addressed Some Limitations	24
	Conclusions	32
	Recommendations	33
	Agency Comments and Our Evaluation	34
<hr/>		
Appendix I: Objectives, Scope, and Methodology		36
Appendix II: Status of Our Prior Identity Theft Refund Fraud Recommendations		39
Appendix III: Comments from the Internal Revenue Service		44
Appendix IV: GAO Contact and Staff Acknowledgments		49
	GAO Contact	49
	Staff Acknowledgments	49
<hr/>		
Appendix V: Accessible Data	50	
	Agency Comment Letter	50
	Data Tables/Accessible Text	55
<hr/>		
Related GAO Products	56	
<hr/>		
Tables		
	Table 1: Extent That IRS's Identity Theft Refund Fraud Estimates, 2013-2014, Meet Selected Best Practice Characteristics for Cost Estimation	25
	Table 2: Potential Estimates of E-file Rejects Using Different IRS Identity Theft (IDT) Defenses, 2014	30
	Table 3: Prior GAO Recommendations to IRS Related to Identity Theft (IDT) Refund Fraud	39
	Accessible Text for Figure 1: Examples of How Identity Thieves Obtain Personally Identifiable Information	55

---

Data Table for Highlights Figure and Figure 4: IRS Estimates of Attempted Identity Theft Refund Fraud, 2014	55
---	----

---

Figures

Figure 1: Examples of How Identity Thieves Obtain Personally Identifiable Information	5
Figure 2: Example of a Successful Identity Theft Refund Fraud Attempt	8
Figure 3: Illustration of IRS <i>Identity Theft Taxonomy</i>	13
Figure 4: IRS Estimates of Attempted Identity Theft Refund Fraud, 2014	14
Figure 5: Illustration of the Taxpayer Protection Program, Filing Season 2015 <sup>a</sup>	16

---

**Abbreviations**

DOJ	Department of Justice
e-file	electronic filing
<i>GAO Cost Guide Global Report</i>	<i>GAO Cost Estimating and Assessment Guide Refund Fraud and Identity Theft Global Report</i>
HRA	High Risk Authentication
IDT	identity theft
IP PIN	Identity Protection Personal Identification Number
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PII	personally identifiable information
RRP	Return Review Program
<i>Taxonomy</i>	<i>Identity Theft Taxonomy</i>
TIGTA	Treasury Inspector General for Tax Administration
TPP	Taxpayer Protection Program
USDS	United States Digital Service
W-2	Form W-2, <i>Wage and Tax Statement</i>

---

---

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



May 24, 2016

The Honorable Orrin Hatch  
Chairman  
The Honorable Ron Wyden  
Ranking Member  
Committee on Finance  
United States Senate

The Honorable Susan M. Collins  
Chairman  
Special Committee on Aging  
United States Senate

The Honorable Kevin Brady  
Chairman  
Committee on Ways and Means  
House of Representatives

The Honorable Bill Nelson  
United States Senate

Identity theft (IDT) refund fraud is an evolving and costly problem that causes hardship for legitimate taxpayers who are victims of the crime and demands an increasing amount of the Internal Revenue Service's (IRS) resources. IDT refund fraud occurs when a refund-seeking fraudster obtains an individual's Social Security number, date of birth, or other personally identifiable information (PII) and uses it to file a fraudulent tax return seeking a refund.<sup>1</sup> This crime burdens honest taxpayers because authenticating their identities is likely to delay the processing of their returns and refunds. IRS estimates that while it prevented or recovered

---

<sup>1</sup>This report discusses IDT refund fraud and not employment fraud. IDT employment fraud occurs when an identity thief uses a taxpayer's name and Social Security number to obtain a job.

---

\$22.5 billion in attempted IDT fraud in 2014, it paid \$3.1 billion in IDT refunds.<sup>2</sup>

According to IRS, a recent data breach at IRS highlights the challenge to the agency—from January 2014 to May 2015, fraudsters were able to use PII to access IRS’s Get Transcript Internet service and obtain tax transcripts containing taxpayers’ tax account information.<sup>3</sup> According to IRS, fraudsters could use that information to more easily create fraudulent returns that would resemble authentic tax returns, making it more difficult for IRS to detect potential fraud. Given current and emerging risks, in 2015 we added IRS’s efforts to address IDT refund fraud to our high-risk area for enforcement of tax laws.<sup>4</sup>

This is our third report on IDT refund fraud since 2014.<sup>5</sup> We previously reported that IRS had undertaken substantial research efforts to combat this problem, such as estimating the cost of IDT refund fraud. These and ongoing efforts included evaluating whether IRS’s methods for authenticating suspicious returns provide reasonable assurance that the authentication determination is accurate and examining the size of the problem. Such work helps IRS continue to adapt as it confronts new and evolving schemes.

Within this context, you asked us to continue examining IRS’s efforts to combat IDT refund fraud. This report (1) evaluates the performance of IRS’s Taxpayer Protection Program (TPP), which reviews returns that are

---

<sup>2</sup>Because of the difficulties in estimating the amount of undetectable fraud, the actual amount could differ from these estimates. IRS’s 2014 estimates cannot be compared to 2013 estimates because of substantial methodology changes to better reflect new IDT refund fraud schemes and to improve the accuracy of its estimates, according to IRS officials.

<sup>3</sup>Tax transcripts provide taxpayers with their tax account transactions or line-by-line tax return information for a specific tax year.

<sup>4</sup>We added this area to the High Risk List by expanding the high risk area of enforcement of tax laws. See GAO, *High Risk Series: An Update*, [GAO-15-290](#) (Washington, D.C.: Feb. 11, 2015).

<sup>5</sup>GAO, *Identity Theft and Tax Fraud: Enhanced Authentication Could Combat Refund Fraud but IRS Lacks an Estimate of Costs, Benefits and Risks*, [GAO-15-119](#) (Washington, D.C.: Jan. 20, 2015) and *Identity Theft: Additional Actions Could Help IRS Combat the Large, Evolving Threat of Refund Fraud*, [GAO-14-633](#) (Washington, D.C.: Aug. 20, 2014).

---

flagged as suspicious by IRS's automated IDT filters; and (2) assesses IRS's efforts to improve its estimates of IDT refund fraud costs for 2014.

To evaluate the performance of TPP, we reviewed IRS studies designed to identify and support ongoing identity authentication refinements.<sup>6</sup> We compared specifics of TPP against relevant guidance on enterprise risk management, electronic authentication, and internal controls.<sup>7</sup> To assess IRS's analysis of TPP's effectiveness, we (1) reviewed relevant IRS documentation, (2) conducted manual testing to identify obvious errors, and (3) interviewed IRS officials. We found IRS did not include all relevant returns in its TPP analysis. To assess how excluding potential IDT refunds affected IRS's TPP estimates of the number of fraudsters able to pass TPP authentication and the IDT refunds issued, we conducted a scenario analysis.

To assess IRS's efforts to improve its 2014 estimates of IDT refunds prevented and paid from previous years, we reviewed *IRS's Identity Theft Taxonomy (Taxonomy)*, which is IRS's estimate of the number and dollar amounts of IDT refunds paid and IDT refunds prevented or recovered in a given calendar year. Specifically, we reviewed the Taxonomy's methodology for 2014, and evaluated it against selected best practices in the *GAO Cost Estimating and Assessment Guide (GAO Cost Guide)* that were applicable to the *Taxonomy*.<sup>8</sup> These best practices are relevant because the Taxonomy is an estimate of the amount of revenue lost to IDT refund fraud—a cost to taxpayers. We also reviewed our past findings and recommendations related to the *Taxonomy* and interviewed

---

<sup>6</sup>IRS Office of Compliance Analytics, *IRS Response to GAO TPP Questions*, (Dec. 16, 2015); *Taxpayer Protection Program Identity Authentication Analytics Update*, (Mar. 23, 2015); *TPP Authentication Analytics Executive Update* (Feb. 18, 2015); and *Taxpayer Protection Program Authentication Analysis Summary from Year 2014*, (February 2015).

<sup>7</sup>IRS, *Internal Revenue Service Enterprise Risk Management Program: Concept of Operations*, (Washington, D.C., May 18, 2015); National Institute of Standards and Technology, *Electronic Authentication Guideline*, Special Publication 800-63-2, (August 2013); Office of Management and Budget, *E-Authentication Guidance for Federal Agencies*, M-04-04 (Washington, D.C.: Dec. 16, 2003); and GAO, *Standards for Internal Control in the Federal Government*, [GAO/AIMD-00-21.3.1](#) (Washington, D.C.: Nov. 1, 1999).

<sup>8</sup>GAO, *GAO Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs*, [GAO-09-3SP](#) (Washington, D.C.: March 2009).

---

IRS officials.<sup>9</sup> We focused our analysis in this report on those best practices that we assessed as “partially met” or less in our review of the 2013 *Taxonomy*.<sup>10</sup> In comparing estimates with 2013 estimates, we could not determine if differences in the estimates were due to changes in methodology, IDT fraud trends, or the efficacy of IRS’s IDT defenses. We also conducted manual data tests, reviewed coding used in the *Taxonomy* estimates for obvious errors, and compared underlying *Taxonomy* data to IRS’s *Refund Fraud & Identity Theft Global Report* to test the reliability of IRS’s *Taxonomy* estimates. Appendix I explains our scope and methodology and provides a summary of best practices selected.

We conducted this performance audit from March 2015 to May 2016 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

---

## Background

---

### Key Components of IDT Refund Fraud

Viewed broadly, IDT refund fraud is composed of two crimes: (1) the theft or compromise of PII, and (2) the use of stolen (or otherwise compromised) PII to file a fraudulent tax return and collect a fraudulent refund.

**Identity theft.** The sources of stolen identities are limitless, according to an official in IRS’s Criminal Investigation Division. Identity thieves can hack into government or commercial systems, recruit insiders (such as employees in the healthcare or education industries) to steal PII, or purchase or put pieces of PII together to create an identity (see figure 1).

---

<sup>9</sup>See [GAO-15-119](#) for our past findings and recommendations related to the *Taxonomy* estimates.

<sup>10</sup>[GAO-15-119](#). See appendix I for a description of the definitions we used to develop our assessment rating for each best practice.

To successfully commit identity theft, thieves can exploit specific digital, physical, or social vulnerabilities (see sidebar). According to Department of Justice (DOJ) officials, the PII used in tax refund fraud can also involve compromised identities, where the real identity holder initially sells his identity to third parties.

**Identity Theft and Personally Identifiable Information (PII) Vulnerability: An Overview**

PII is vulnerable to theft and exploitation in three broad areas.

**Digital vulnerability:** Criminals can access large amounts of digital information if it is inadequately safeguarded. For example, thieves can steal it through hacking and computer intrusion, can aggregate publicly available information, or can sell and buy PII from other criminals on the black market. In one case, a foreign national obtained PII from online databases and sold it to other criminals, resulting in 13,673 victims and \$65 million claimed in refund fraud.

**Physical vulnerability:** If insufficient attention is paid to the structures and tools used to store, maintain, and safeguard PII, such as hard drives, paper records, or unsecured mailboxes, thieves will exploit these vulnerabilities through computer theft and "dumpster diving."

**Social vulnerability:** Thieves can trick individuals into divulging their own PII or others' PII, for example by impersonating IRS officials. Thieves may also recruit individuals with legitimate access to sensitive information. In one case, a ring of thieves used its employment access to steal identities from public and private databases, such as the U.S. Army, several Alabama state agencies, a Georgia call center and employee records from a Georgia company.

Source: Internet Criminal Complaint Center and GAO analysis of Department of Justice and Federal Trade Commission documents. | GAO-16-508

**Figure 1: Examples of How Identity Thieves Obtain Personally Identifiable Information**



Source: GAO analysis | GAO-16-508

Thieves can use the information for criminal purposes or sell PII on the black market to other criminals who then use it to commit crimes, according to officials at DOJ and the IRS Criminal Investigations Division. Criminals can use stolen or compromised PII to commit a number of crimes, including financial crimes (such as IDT refund fraud and credit card fraud) or crimes against national security (such as selling falsified identity documents).

As advances in technology have allowed the government and businesses to collect extensive amounts of PII, cyber security has become a growing concern. Businesses and federal agencies alike have had high-profile breaches of PII in recent years. From fiscal years 2006 to 2014, federal agencies reported a 1,121 percent increase in the number of information security incidents (from 5,503 to 67,168). We have designated federal

---

information security as a government-wide, high-risk area since 1997. In 2015, we expanded this area to include protecting the privacy of personally identifiable information that is collected, maintained, and shared by both federal and nonfederal entities.<sup>11</sup>

As mentioned earlier, IRS's systems were targeted from January 2014 through May 2015, when criminals exploited IRS's Internet tax transcript service, Get Transcript, to obtain PII. IRS has since suspended the service. In June 2015, the Commissioner of the IRS testified that criminals used taxpayer-specific data acquired from non-IRS sources to gain unauthorized access to tax transcripts, which contain information on taxpayers' prior year tax return information.<sup>12</sup> In February 2016, after further investigation, IRS and the Treasury Inspector General for Tax Administration (TIGTA) confirmed, in total, that fraudsters gained unauthorized access on about 724,000 taxpayer accounts. IRS and TIGTA reported an additional 576,000 attempts failed to clear IRS's authentication processes.<sup>13</sup> According to IRS officials, with access to tax transcripts, fraudsters can create historically consistent returns that are hard to distinguish from a return filed by a legitimate taxpayer. This potentially makes it more difficult for IRS to identify and detect IDT refund fraud. In response to our concerns about the increased vulnerabilities presented by the Get Transcript incident, IRS enhanced its IDT filters and is working toward instituting new authentication procedures to further protect the refunds of affected tax accounts.

Given fraudsters' access to PII and the importance of prerefund preventative controls to help defend against invalid refunds, it is important that IRS is able to discern legitimate taxpayers from fraudsters. We previously reported that IRS is pursuing improved taxpayer authentication to prevent IDT refund fraud, but did not have a plan to assess costs, benefits, and risks. Thus, we recommended that IRS assess the costs, benefits, and risks of various authentication tools the agency could use to better identify legitimate taxpayers from fraudsters. In April 2015, IRS

---

<sup>11</sup>[GAO-15-290](#).

<sup>12</sup>John A. Koskinen, Commissioner of the Internal Revenue Service, *Unauthorized Attempts to Access Taxpayer Data*, testimony before the Senate Committee on Homeland Security and Governmental Affairs, 114<sup>th</sup> Cong., 1<sup>st</sup> sess., June 2, 2015.

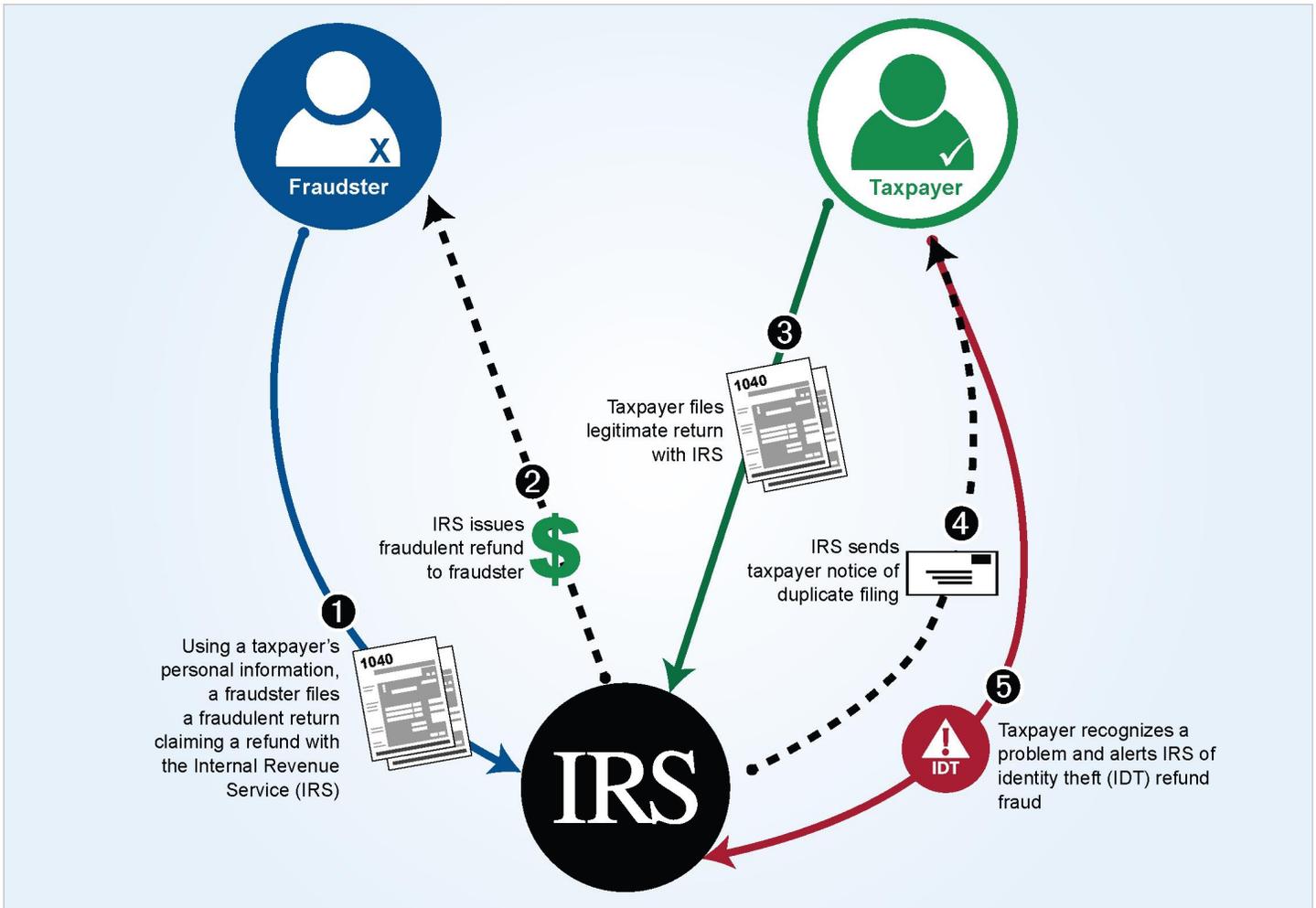
<sup>13</sup>Internal Revenue Service, *IRS Statement on "Get Transcript"* (Feb. 26, 2016).

---

reported that it would implement our recommendation. (See appendix II for the status of related prior recommendations).

**Using stolen PII to commit tax refund fraud.** Figure 2 presents an example of how fraudsters may use stolen PII and other information, real or fictitious (e.g., sources and amounts of income), to complete and file a fraudulent tax return. Fraudsters can obtain fraudulent refunds via a paper check, direct deposit into a bank account, or a general purpose reloadable card—also known as a prepaid debit card. For example, in a press release issued in 2014, DOJ reported that a fraudster obtained refunds on prepaid cards and then recruited several individuals to make withdrawals at numerous locations and to later provide the fraudster with cash. According to the press release, the fraudster admitted to possessing more than 600 people’s PII and 200 prepaid debit cards.

**Figure 2: Example of a Successful Identity Theft Refund Fraud Attempt**



Source: GAO analysis. | GAO-16-508

Note: This figure's numbering shows the order in which events occur when fraudsters successfully commit IDT refund fraud.

As we previously reported, IDT refund fraud takes advantage of the timing of IRS's compliance process.<sup>14</sup> IRS issues refunds after performing selected reviews, such as verifying identities by matching names and

<sup>14</sup>GAO-14-633.

---

Social Security numbers, and filtering for indications of fraud.<sup>15</sup> However, the wage information that employers report on the *Form W-2, Wage and Tax Statement* (W-2), has generally been unavailable to IRS until after it issues most refunds. As a result, IRS generally cannot match third-party information returns (such as W-2s) to tax returns prior to issuing refunds.<sup>16</sup> With earlier access to W-2 data, IRS could match and validate information reported on a tax return (e.g., wages and compensation) with information reported by employers before issuing refunds.

In certain instances, IRS requests W-2 information from employers to validate information on returns selected by fraud filters. Consistent with IRS's reported strategy for incorporating earlier W-2 information to detect IDT refund fraud, IRS officials stated that IRS had incorporated earlier W-2 data into its Return Review Program (RRP) for filing season 2016 where data are available.<sup>17</sup>

Consistent with our prior recommendations, the Consolidated Appropriations Act, 2016, amended the tax code to accelerate W-2 filing deadlines to January 31 starting in 2017.<sup>18</sup> This change will provide IRS with earlier access to W-2 data. According to IRS, prerefund matching would potentially save a substantial part of the billions of taxpayer dollars currently lost to fraudsters. (See appendix II for information on our prior recommendations related to prerefund W-2 matching.)

A recent scheme highlights that even prerefund matching to W-2s is no silver bullet, as criminals adapt to IRS's new fraud defenses. For example, in March 2016, IRS alerted payroll and human resource professionals of a new phishing e-mail scheme where fraudsters pose as company executives requesting personal information on employees,

---

<sup>15</sup>These reviews can detect inconsistencies, allowing IRS to resolve any issues and—in some cases—prevent refunds.

<sup>16</sup>Third parties—employers, banks, and others—report wages, interest, and other information to both taxpayers and IRS.

<sup>17</sup>RRP is intended to be a web-based automated system designed to enhance IRS's capabilities to detect, resolve, and prevent criminal and civil noncompliance.

<sup>18</sup>Pub. L. No. 114-113, div. Q, § 201, 129 Stat. 2242 (Dec. 18, 2015). This change goes into effect for W-2s reporting payments made in 2016 and filed in 2017. See [GAO-14-633](#) for our recommendations related to W-2 matching.

---

including W-2s. Fraudsters then have the potential to use this information to imitate the legitimate taxpayer and file fraudulent tax returns seeking refunds.

According to DOJ officials, another IDT refund scheme involves using Puerto Rican identities to commit tax refund fraud. DOJ officials further stated that because Puerto Rican U.S. citizens typically do not have a filing obligation, detecting fraud is difficult because the real owner of the Social Security number is unlikely to file a U.S. tax return. In one scheme, conspirators used PII of Puerto Ricans and other individuals to obtain more than \$2.5 million in IDT refunds.

---

## IRS's IDT Refund Fraud Response

IRS recognized the challenge of IDT refund fraud in its fiscal year 2014-2017 strategic plan and increased resources dedicated to combating IDT and other types of refund fraud.<sup>19</sup> In fiscal year 2015, IRS reported that it staffed more than 4,000 full-time equivalents and spent about \$470 million on all refund fraud and IDT activities.<sup>20</sup> The administration requested an additional \$90 million and 491 full-time equivalents for fiscal year 2017 to help prevent IDT refund fraud and reduce improper payments.<sup>21</sup> IRS estimates that this \$90 million would help it protect an additional \$612 million in revenue in fiscal year 2017, as well as protect revenue in future years. The Consolidated Appropriations Act, 2016, appropriated IRS an additional \$290 million for improvements to customer service, IDT identification and prevention, and cybersecurity efforts. The IRS spending plan indicates that officials will use this funding to (1) reduce the wait times and improve the performance on IRS's Taxpayer Protection Program/Identity Theft Toll Free Line, and (2) improve network security and protect taxpayer data from unauthorized access by identity thieves, among other things.

---

<sup>19</sup>IRS, *Strategic Plan: FY2014-2017*, (Washington, D.C.: June 2014).

<sup>20</sup>IRS officials told us they do not track spending for identity theft activities separately from other types of refund fraud. A full-time equivalent reflects the total number of regular straight-time hours (i.e., not including overtime or holiday hours) worked by employees divided by the number of compensable hours applicable to each fiscal year.

<sup>21</sup>Improper payments are payments that should not have been made or that were made in an incorrect amount (including overpayments and underpayments).

---

To detect and prevent IDT refund fraud, IRS has developed tools and programs, including:<sup>22</sup>

- **IDT filters:** IRS uses automated filters that search for IDT refund fraud characteristics to identify suspicious returns during processing and to confirm taxpayers' identities before issuing refunds. These characteristics are based on both IRS's knowledge of previous refund fraud schemes and clusters of returns with similar characteristics.
- **Taxpayer Protection Program.** The Taxpayer Protection Program (TPP) reviews returns that are flagged by IRS's IDT filters. IRS asks taxpayers to authenticate their identities—either online or by phone—by answering questions that a legitimate taxpayer is likely to know, such as previous addresses, mortgage information, and data about family members. If the taxpayer fails to authenticate himself online or by phone, IRS instructs the respondent to authenticate his identity in person at an IRS Taxpayer Assistance Center.
- **Identity Protection Personal Identification Number (IP PIN):** IP PINs are single-use identification numbers sent to IDT victims who have authenticated their identities with IRS. If a return is electronically filed (e-filed) for a Social Security Number assigned an IP PIN, it must include the IP PIN or else IRS will reject the return. If a paper return has a missing or incorrect IP PIN, IRS delays processing the return while the agency determines if it was filed by the legitimate taxpayer. As a result of an ongoing security review, IRS temporarily suspended the IP PIN tool in March 2016 while it assesses how to further strengthen its security features.<sup>23</sup>

IRS also works with third parties, such as industry, states, and financial institutions, to try to detect and prevent IDT refund fraud. In March 2015, the IRS Commissioner convened a Security Summit with industry and states to improve information sharing and authentication. IRS officials said that 40 state departments of revenue and 20 tax industry participants have officially signed on to the partnership. IRS is investing \$16.1 million for identity theft prevention and refund fraud mitigation actions that come

---

<sup>22</sup>For details on IRS's IDT tools for identifying and combating IDT refund fraud, see [GAO-14-633](#) and [GAO-15-119](#).

<sup>23</sup>The IP PIN tool allows taxpayers who have lost their IP PINs to retrieve their numbers online.

---

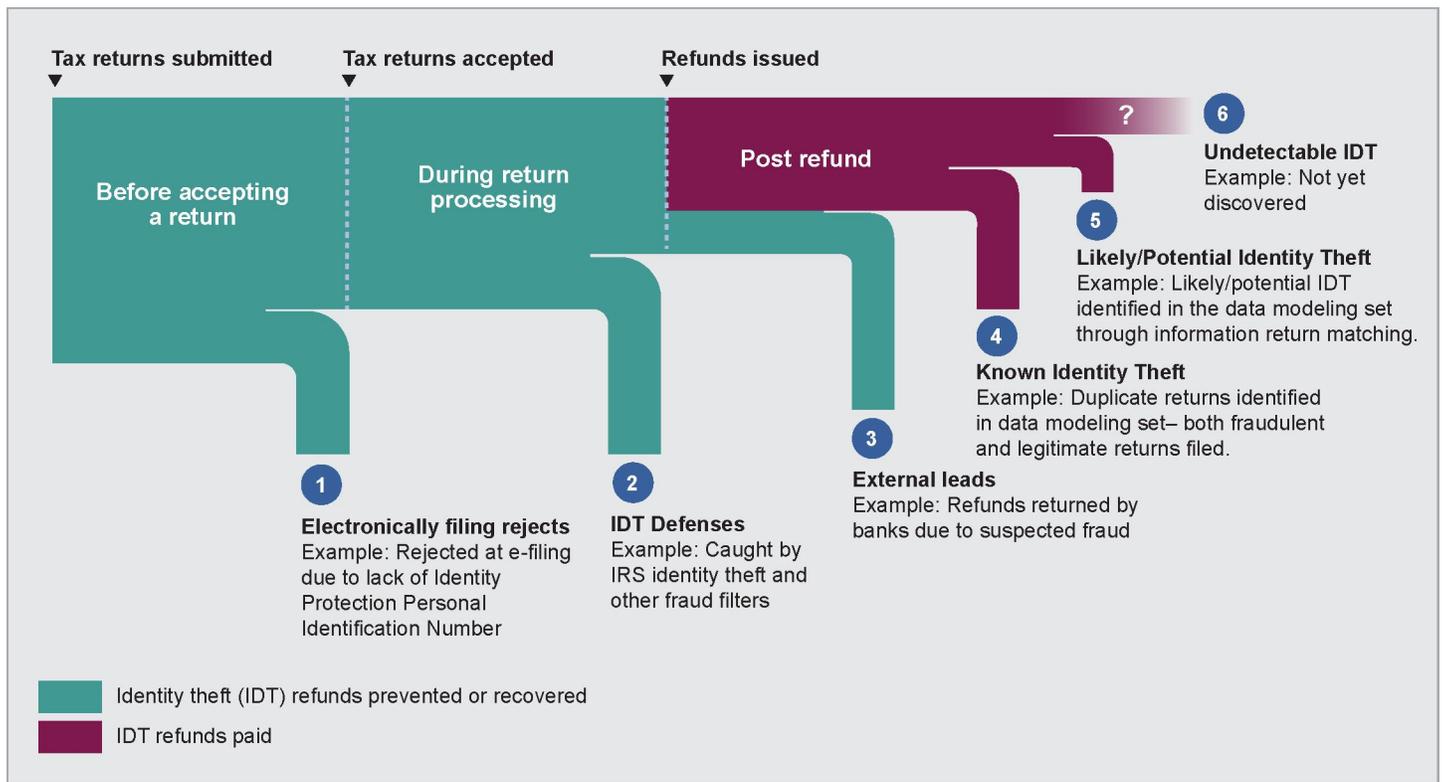
out of the Security Summit. These efforts include developing an Information Sharing and Analysis Center where IRS, states, and industry can share information to combat IDT refund fraud.

---

### How IRS Estimates the Extent of IDT Refund Fraud

IRS monitors the extent of IDT refund fraud through its *Taxonomy*. This research-based effort aims to report on the effectiveness of IRS's IDT defenses to internal and external stakeholders, help IRS identify IDT trends and evolving risks, and refine IDT filters to better detect potentially fraudulent returns, while reducing the likelihood of flagging legitimate tax returns. As shown in figure 3, IRS's *Taxonomy* estimates the number of identified IDT refund fraud cases where IRS (1) prevented or recovered the fraudulent refunds (turquoise band), and (2) paid the fraudulent refunds (purple band). IRS breaks these estimates into categories corresponding to IDT detection strategies, which occur at three key points in the life cycle of a tax refund: before accepting a tax return, during return processing, and post refund.

**Figure 3: Illustration of IRS *Identity Theft Taxonomy***



Source: GAO analysis of *IRS Taxonomy*. | GAO-16-508

IRS creates the *Taxonomy's* estimates through sources including *IRS's Refund Fraud & Identity Theft Global Report (Global Report)* and a modeling data set composed of known IDT returns and potential identity theft returns.<sup>24</sup> In response to our recommendation in January 2015, IRS began using the modeling data set to improve *Taxonomy* estimates for refunds it paid (Categories 4 and 5 in figure 3 above).<sup>25</sup> According to IRS officials, the agency developed its modeling data set to explore IDT characteristics and build the models within its IDT filters to help identify

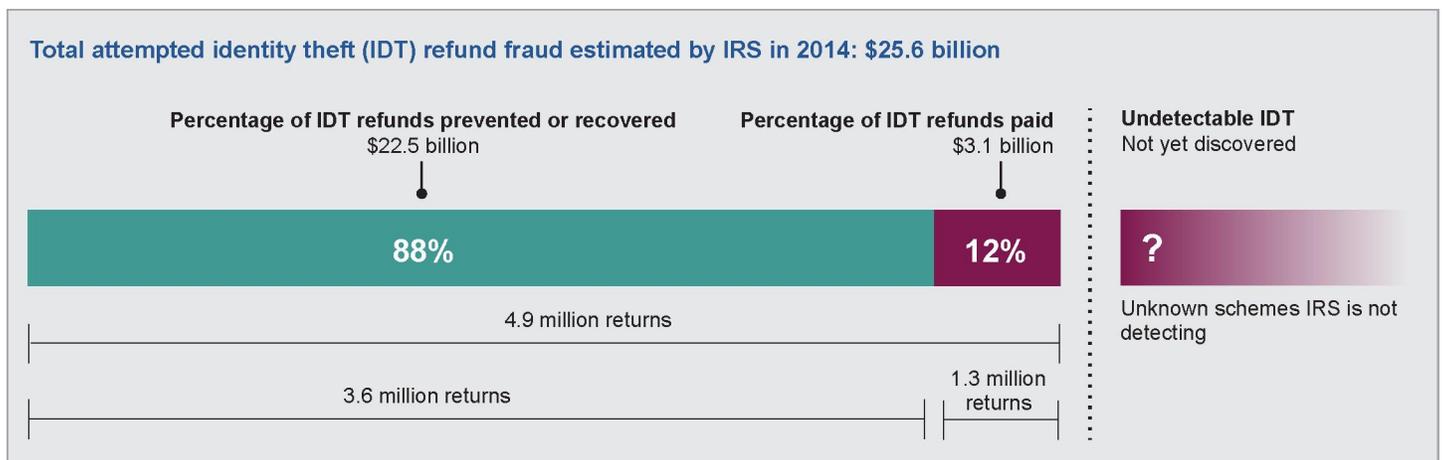
<sup>24</sup>IRS developed the internal *Global Report* in July 2012 to consolidate, aggregate, and track IRS's existing information about identity theft incidents. IRS uses the report to provide information to senior management and to provide a standard source of information for responding to data requests from external entities, according to IRS officials.

<sup>25</sup>GAO-15-119.

and protect against IDT refund fraud. The modeling data set consolidates data on known and potential IDT returns from various IRS systems and programs.

Figure 4 shows IRS’s estimates of attempted IDT refund fraud for 2014. IRS estimates that it prevented or recovered \$22.5 billion in IDT refunds. For the cost of IDT refunds paid, IRS estimated a range of values; the \$3.1 billion estimate for IDT refunds paid represents the upper bound of IRS’s range for IDT refunds paid. However, IRS recognizes that there is imprecision in these estimates.<sup>26</sup> Further, there is uncertainty in these estimates, as will be discussed later.<sup>27</sup>

**Figure 4: IRS Estimates of Attempted Identity Theft Refund Fraud, 2014**



Source: GAO analysis of IRS data. | GAO-16-508

<sup>26</sup>Further analysis by IRS found that a more precise estimate of IDT refunds paid to fraudsters is \$2.4 billion to \$2.7 billion for 2014. However, we are not confident in IRS’s methodology for calculating this range. According to IRS officials, they report the \$3.1 billion as the official estimate for IDT refunds because it is the “worst case scenario” of the estimated amount of IDT refund fraud.

<sup>27</sup>Uncertainty refers to a situation in which little to no information is known about the outcome.

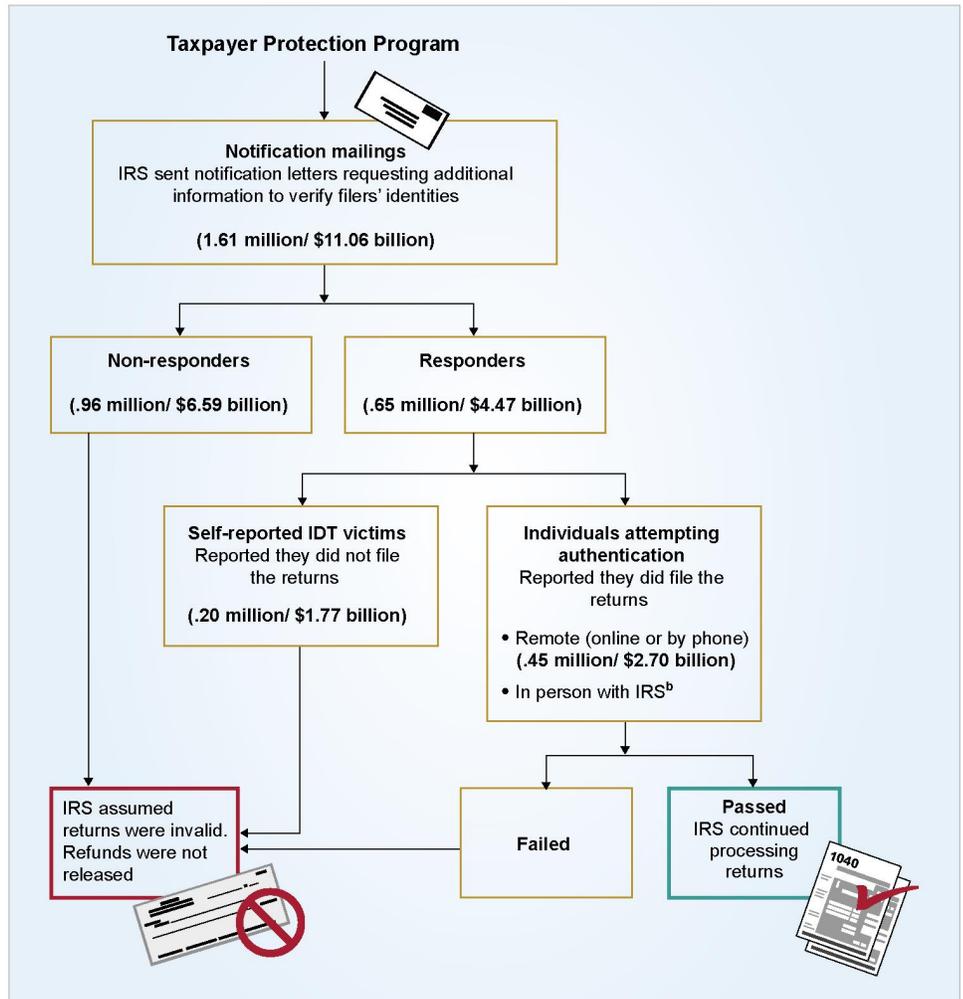
---

---

## Despite Recent Changes, Vulnerabilities in the Taxpayer Protection Program Limit IRS's Ability to Prevent IDT Refund Fraud

One of IRS's key defenses in reducing the risk of IDT refund fraud is TPP, which is intended to verify the identities of suspicious filers. TPP has procedures that help IRS authenticate legitimate taxpayers by requiring filers to answer questions only legitimate taxpayers are likely to know, or in some instances, checking information reported on filers' returns with information reported by third parties, such as W-2s. Figure 5 illustrates the TPP process.

**Figure 5: Illustration of the Taxpayer Protection Program, Filing Season 2015<sup>a</sup>**



Source: GAO analysis. | GAO-16-508

Note: These estimates may be lower than actual numbers due to data limitations. For example, estimates do not include data for TPP selections where filers attempted authentication only in person at Taxpayer Assistance Centers because IRS does not have detailed return-level data for these filers. IRS estimates that about 100,000 filers only attempted authentication at a Taxpayer Assistance Center, though this may overcount instances where the same taxpayer attempted in-person authentication multiple times. The estimates also do not account for the approximately 144,000 returns that received refunds after IRS confirmed that information reported on the tax returns matched information returns provided by third parties. Based on IRS data, it is unclear which of these returns filers may have attempted to authenticate online or by phone before receiving information return releases.

<sup>a</sup>Data are as of October 7, 2015. Totals may not add due to rounding.

<sup>b</sup>Data are unavailable for filers who attempted to authenticate TPP selections in person.

---

Of the 650,000 filers who responded to TPP notification letters, 450,000 (69 percent) attempted remote authentication—online or by phone—whereas 200,000 (31 percent) claimed to be victims of IDT who had not filed the selected returns. To pass remote authentication, filers first complete “identity proofing” by providing basic identifying information such as their names and dates of birth. Next, they are asked to answer knowledge-based authentication questions obtained from a third-party provider. Examples of authentication questions are “Who is your mortgage lender?” or “Which of the following is your previous address?” If filers pass knowledge-based remote authentication, then IRS releases those filers’ returns for further processing before issuing refunds. If filers cannot pass, IRS will not issue a refund unless those filers pass in-person authentication or IRS receives information return documents from third parties, such as W-2s, that match filers’ return data.

Officials stated that TPP authentication poses a challenge to IRS because it must authenticate almost all taxpayers in the program remotely. According to a United States Digital Service (USDS) report, it is costly for fraudsters to attempt in-person authentication at scale because it requires human interaction.<sup>28</sup> As a result, when compared to in-person authentication, fraudsters are incentivized to remotely authenticate because it allows for multiple attempts, allowing the fraudster more opportunity to access the taxpayers’ information more quickly and easily respond to authentication questions.<sup>29</sup>

---

## IRS Strengthened TPP Phone Authentication Procedures for the 2015 Filing Season

IRS has conducted research both to evaluate the effectiveness of existing TPP authentication procedures and to identify options for strengthening those procedures. Based on research efforts, IRS made improvements to its phone authentication options for filing season 2015. For example, IRS created a more challenging High Risk Authentication (HRA) quiz, which requires taxpayers to recall information from past tax filings. Prior to the 2015 filing season, IRS’s HRA quizzes sometimes included simulated questions where IRS effectively had no data available to support correct

---

<sup>28</sup>The U.S. Digital Service, *USDS IRS Discovery Sprint Report* (Oct. 30, 2015).

<sup>29</sup>While IRS allows filers to attempt remote TPP authentication multiple times, IRS places limits on the number and frequency of remote authentication attempts. This helps restrict IDT fraudsters’ opportunities to pass remote authentication.

---

answers other than “none of the above.” For example, a simulated question might ask a filer to identify the date of birth of a dependent even though that filer had no dependent. For the 2015 filing season, IRS eliminated these questions from HRA quizzes. IRS analysis has shown that simulated questions are easier to pass than questions based on taxpayer data. In addition, IRS required some respondents to answer a higher proportion of HRA questions correctly in the 2015 filing season.

---

**While TPP Protects Billions in Revenue, Some IDT Fraudsters Pass TPP Authentication and Potentially Receive Millions in Fraudulent Refunds**

Of the about 1.6 million returns selected for TPP processing in filing season 2015, IRS estimated that it potentially paid about \$30 million to IDT fraudsters who filed about 7,200 returns that passed TPP authentication.<sup>30</sup> However, our analysis indicates that IRS underestimated how many fraudulent IDT returns passed TPP authentication.

In developing its estimates, IRS first compared TPP selections to information returns provided by third parties, such as W-2s. IRS next identified which TPP selections passed authentication but had large mismatches with information returns. IRS then manually reviewed a sample of these returns to approximate how many returns that passed authentication were filed by likely IDT fraudsters.<sup>31</sup> IRS used this finding to estimate the total number and value of refunds potentially paid to IDT fraudsters who passed TPP authentication.

IRS likely underestimated how many fraudulent IDT returns passed TPP authentication because the agency did not include potential IDT returns that closely matched information returns. Though based on a

---

<sup>30</sup>In 2015, IRS processed more than 150 million individual tax returns. The 1.6 million returns selected for TPP processing is based on our analysis of IRS data, which is presented in figure 5. This estimate does not account for TPP selections that passed authentication after IRS received matching information returns. It also does not include selections in which filers only attempted to authenticate in person. This time frame corresponds to tax year 2014. IRS’s TPP analyses are a separate research effort from the *Taxonomy* estimates of IDT refund fraud. Further, they are not comparable to the *Taxonomy* because the analyses cover different time periods.

<sup>31</sup>Based on its review, IRS determined that some mismatching returns were filed by legitimate taxpayers, though some appeared to involve other types of fraud, such as an individual who submitted a fraudulent return using his or her own identity. To distinguish IDT fraud returns from non-IDT fraud returns, IRS examiners evaluated returns according to a variety of characteristics such as consistency of occupation across filing seasons.

---

nongeneralizable sample, past IRS research suggests that some IDT fraudsters are able to both file tax returns that closely match information provided by third parties and pass TPP authentication.<sup>32</sup> By omitting some IDT returns from its estimates, IRS likely overestimated the effectiveness of TPP defenses. IRS officials told us that they did not include close matches in their analysis because it is challenging to determine how many of these returns are filed by IDT fraudsters, and IRS does not want to present estimates based on assumptions that could be inaccurate. In March 2016, IRS officials acknowledged the desirability of expanding their estimate to include a more generalizable sample of those who successfully passed authentication and said that they will consider doing so as staff are available to do so after the filing season.

While we cannot quantify the specific amount by which IRS's analysis underestimated the number of fraudulent IDT returns that passed TPP authentication, we conducted a scenario analysis to demonstrate the effect of omitting potential IDT returns on IRS's estimates. If we assume that 5 to 10 percent of close matches passing authentication were filed by potential IDT fraudsters, we estimate that the value of refunds potentially paid to IDT fraudsters who passed TPP authentication could be as high as between \$116 and \$203 million in the 2015 filing season. We chose to not base our analysis on IRS's past research (cited in the previous paragraph) because it used a nongeneralizable sample and because its methodology for identifying close matches changed from 2014 to 2015. Our analysis indicates that, even if a small proportion of close matches that pass TPP authentication are filed by IDT fraudsters, accounting for these selections can substantially affect IRS's estimates because close matches represent about 91 percent of all returns filed by individuals who passed authentication. Further, the extent of IRS's likely underestimation suggests that TPP's authentication procedures may be at greater risk of exploitation by IDT fraudsters than suggested by IRS's estimates.

---

<sup>32</sup>IRS Office of Compliance Analytics, *Taxpayer Protection Program Authentication Analysis Summary from Year 2014*, (February 2015).

---

## TPP Uses Remote Authentication Procedures That Some Fraudsters Can Pass

To verify taxpayers' identities remotely, TPP uses single-factor authentication procedures that incorporate one of the following authentication elements: "something you know," "something you have," or "something you are."<sup>33</sup> TPP's single-factor authentication procedures are at risk of exploitation because some fraudsters obtain the PII necessary to pass the questions asked during authentication. According to IRS officials, criminals can find personal information needed to pass authentication by searching records available through the Internet or purchasing it from websites designed to conceal their content. USDS has also reported that implementing effective authentication procedures has become more challenging because criminals are able to pass authentication checks at similar rates to legitimate users due to the wide availability of personal information.<sup>34</sup>

Similar to TPP, IRS used single-factor authentication procedures to authenticate users of its Get Transcript service, which fraudsters defeated in 2014 to 2015, as well as its IP PIN tool that IRS temporarily suspended due to security concerns in 2016. Both USDS and TIGTA have found that IRS needs to take a stronger approach to authenticating Get Transcript users.<sup>35</sup> Though IRS is undertaking efforts to strengthen Get Transcript authentication, agency officials said they are still working to determine if improvements are necessary for TPP.

Because IRS must ensure legitimate taxpayers can successfully authenticate, the agency faces challenges in making remote authentication more difficult for IDT fraudsters who often possess the PII needed to appear to be legitimate taxpayers. IRS officials said it was important for TPP to minimize delays in refund processing for large numbers of legitimate taxpayers and to avoid the appearance of discriminating against specific types of filers. For example, IRS could

---

<sup>33</sup>TPP's identity proofing and knowledge-based authentication quizzes challenge filers to provide "something they know." An example of "something you have" could be a driver's license, while "something you are" could be a fingerprint. National Institute of Standards and Technology, *Electronic Authentication Guideline, NIST Special Publication 800-63-2* (August 2013).

<sup>34</sup>The U.S. Digital Service, *USDS IRS Discovery Sprint Report* (Oct. 30, 2015).

<sup>35</sup>The U.S. Digital Service, *USDS IRS Discovery Sprint Report* (Oct. 30, 2015) and TIGTA, *Improved Tax Return Filing and Tax Account Access Authentication Processes and Procedures are Needed*, 2016-40-007 (Nov. 19, 2015).

---

designate all TPP filers whose return information may be harder to verify for more challenging authentication; however, IRS officials said the agency wanted to avoid the appearance of discriminating against these filers who, on average, report lower income. In addition, IRS could delay refunds for these respondents until IRS could match these selections' return data against information provided by third parties. Because delaying refunds is likely to burden taxpayers, IRS officials said large-scale delays were not feasible.

---

### IRS's Most Recent Risk Assessment May Not Reflect the Threat That IDT Refund Fraud Currently Poses to TPP Authentication Procedures

Although IRS conducted a risk assessment for TPP authentication in October 2012, the agency has not updated this assessment to reflect the current threat of IDT refund fraud—specifically, the threat that some fraudsters possess the PII necessary to pass authentication questions.<sup>36</sup> In conducting its risk assessment, IRS determined that improper authentication through TPP posed low or moderate risks to both the agency and taxpayers, and therefore required no more than single-factor authentication.<sup>37</sup> Since IRS conducted its original risk assessment for TPP, TIGTA conducted a more recent risk assessment of Get Transcript and determined that Get Transcript should have required multi-factor rather than single-factor authentication.<sup>38</sup> Given that both programs pose similar risks—fraudsters can use vulnerabilities in both Get Transcript and TPP to more easily obtain tax refunds—it seems likely that IRS would identify a higher authentication standard for TPP when updating that program's risk assessment. In March 2016, IRS officials stated that they were planning to conduct a risk assessment and make improvements to TPP based on the results. However, their plans for a risk assessment are not documented yet because the Identity Assurance Office has prioritized improving authentication for Get Transcript service and the IP PIN tool before TPP.

---

<sup>36</sup>At the time IRS conducted its risk assessment, the Taxpayer Protection Program included only a phone authentication option whereby responders authenticated through an IRS customer service representative. IRS conducted its risk assessment to determine the risks associated with authentication quizzes completed both by phone and online, although IRS had yet to implement its new online option. Now active, this online option is called "ID Verify."

<sup>37</sup>IRS, *E-authentication Risk Assessment*, (Oct. 1, 2012).

<sup>38</sup>Multi-factor authentication requires at least two of the following authentication elements: "something you know," "something you have," or "something you are."

---

Office of Management and Budget (OMB) e-authentication guidance directs agencies to conduct risk assessments on information technology systems that remotely authenticate users and to identify appropriate assurance levels.<sup>39</sup> Agencies then select authentication technologies based on the levels of assurance needed and e-authentication technical guidance provided by the National Institute of Standards and Technology (NIST).<sup>40</sup> Senior IRS officials stated that they disagreed that OMB guidance and NIST e-authentication standards are applicable to TPP phone authentication. However, we believe the guidance and standards are applicable because TPP uses similar processes (e.g., knowledge-based authentication questions) to remotely authenticate taxpayers—whether taxpayers themselves type in answers to questions online or whether the taxpayer answers the questions over the phone and IRS Customer Service Representatives import the information into an Internet application to check those answers.<sup>41</sup> Following a consistent standard for both online and phone authentication would also help prevent IDT fraudsters from shifting authentication attempts to the option that requires a less rigorous standard.

In addition, federal internal control standards, best practices for risk management, and IRS's own risk management guidance require or recommend that agencies regularly assess risks to their programs. *Standards for Internal Control in the Federal Government* state that

---

<sup>39</sup>OMB, *E-Authentication Guidance for Federal Agencies*, M-04-04 (Washington, D.C.: Dec. 16, 2003). The OMB guidance provides criteria for determining the level of e-authentication assurance appropriate for specific transactions, based on the risks and their likelihood of occurrence of each application or transaction. OMB and National Institute of Standards and Technology guidance defines four levels of assurance. Each assurance level describes the agency's degree of certainty in terms of consequences of authentication errors and misuse of credentials. For example, level 3 provides high confidence in the asserted identity's validity and would require multi-factor authentication (e.g., a username and password plus a token displaying a new personal identification number every minute).

<sup>40</sup>NIST, *Electronic Authentication Guideline, Special Publication 800-63-2* (August 2013).

<sup>41</sup>OMB guidance and NIST guidelines were issued in response to the E-Government Act of 2002. The purpose of the act was to enhance the management and promotion of electronic government services. Electronic government was broadly defined under the act to include web-based Internet applications and other information technologies, combined with the process to implement these technologies. Under TPP, even if the taxpayer calls to authenticate his identity, IRS uses an Internet application to verify the taxpayer's responses to knowledge-based authentication quizzes.

---

agency management should assess the risks that the agency faces from both external and internal sources.<sup>42</sup> Best practices in risk management recommend that fraud risk assessments generally include assessing risks' likelihoods and impacts, determining the agency's risk tolerance, and examining the suitability of existing fraud controls.<sup>43</sup> In addition, they recommend that agencies plan regular fraud risk assessments, since allowing extended periods to pass between assessments could result in control activities that do not effectively address a program's risks. IRS's *Enterprise Risk Management Program: Concept of Operations* also states that IRS's Office of the Chief Risk Officer is likewise committed to timely risk reporting.<sup>44</sup>

By conducting an updated risk assessment for TPP in accordance with e-authentication and risk management standards, IRS could identify appropriate opportunities to strengthen TPP authentication and prevent IDT fraudsters from passing and potentially receiving millions of dollars in refunds. Depending on the assessment's results, IRS could implement stronger authentication procedures. For example, a multi-factor authentication standard for TPP's remote authentication options would utilize a second element to authenticate filers, such as requiring filers to provide proof of "something they have" in addition to testing "what they know."

Strengthening TPP authentication could help IRS prevent millions of dollars from being paid to IDT fraudsters each filing season. In addition, strengthening TPP could improve IRS's return on investment for fraud filters by ensuring that efforts to flag fraudulent returns result in fewer refunds paid to IDT fraudsters. Fewer legitimate taxpayers would also become victims of IDT refund fraud if TPP stopped more IDT refund fraud returns.

---

<sup>42</sup>GAO, *Standards for Internal Control in the Federal Government*, [GAO/AIMD-00-21.3.1](#) (Washington, D.C.: November 1999).

<sup>43</sup>GAO, *A Framework for Managing Fraud Risks in Federal Programs*, [GAO-15-593SP](#) (Washington, D.C.: July 28, 2015).

<sup>44</sup>IRS, *Internal Revenue Service Enterprise Risk Management Program: Concept of Operations* (May 18, 2015).

---

## IRS Improved Its Methodology for *Taxonomy* Estimates, but Has Not Addressed Some Limitations

In response to recommendations made in our previous report, IRS is working to improve *Identity Theft Taxonomy (Taxonomy)* estimates of IDT fraud. In that report, we found that IRS's 2013 *Taxonomy* estimates met several *GAO Cost Estimating and Assessment Guide (GAO Cost Guide)* best practices, such as regularly updating the methodology to better reflect evolving fraud schemes.<sup>45</sup> However, we also found limitations and recommended that IRS improve the estimates by (1) reporting the inherent imprecision and uncertainty of estimates, and (2) documenting the underlying analyses justifying cost-influencing assumptions.<sup>46</sup> IRS reported that the agency is working to implement these recommendations by October 2016.

Given the challenges inherent in estimating fraudulent activity and the evolving nature of fraud schemes, IRS's efforts to improve *Taxonomy* estimates are likely to be ongoing.<sup>47</sup> For example, to estimate potential IDT refund fraud paid, IRS compares the information reported on tax returns with data reported by third parties on information returns, such as Form W-2, *Wage and Tax Statement (W-2)*. However, it is difficult for IRS to determine whether discrepancies between data reported on the tax return and information returns are due to IDT, a mistake made by the legitimate taxpayer, or other types of fraud committed by the legitimate taxpayer. Moreover, IRS cannot accurately estimate amounts of undetected fraud because of situations when it has no reported information to verify income. Furthermore, to better reflect evolving IDT refund fraud schemes, IRS updates the *Taxonomy* methodology over

---

<sup>45</sup>Refund fraud is a cost to taxpayers. While the *Taxonomy* is not a capital program, it is a cost estimate of the amount of IDT refund fraud IRS is preventing and recovering and the IDT refund fraud IRS is paying. We previously determined that the *GAO Cost Guide* is appropriate to use as criteria during our review of the 2013 *Taxonomy*. See [GAO-15-119](#) for more details.

<sup>46</sup>We previously found that IRS did not conduct a risk and uncertainty analysis showing the cumulative effect that assumptions have on 2013 *Taxonomy* estimates. As a result, the level of uncertainty associated with the *Taxonomy* estimates is unclear and users of the estimates may be left with a mistaken impression of their precision.

<sup>47</sup>Developing loss estimates of illicit activities is challenging because such activities are difficult to observe. For this reason, IRS makes various assumptions in calculating *Taxonomy* estimates. Risk and uncertainty analysis recognizes the potential for error and captures the cumulative effect that assumptions have on the cost estimate. It involves using methods to develop a range of costs around a point estimate.

time. While these updates may result in more accurate estimates, these changes confound making comparisons between filing seasons.

To assess IRS's efforts to implement our past recommendations, we reviewed IRS's 2014 estimates focusing on those best practices that we assessed as "partially met" or less in our review of the 2013 *Taxonomy*.<sup>48</sup> While IRS is not required to follow the *GAO Cost Guide* best practices, it could help IRS meet OMB and its own information quality guidelines and improve the reliability of IDT refund fraud estimates.<sup>49</sup> Our assessments—summarized in table 1—note places where IRS has taken steps to improve the estimates and places where IRS can take additional action to further improve its estimates. Our assessment ratings show IRS made progress in one area and took a step back in another area compared to 2013. The ratings remained unchanged in four areas.

**Table 1: Extent That IRS's Identity Theft Refund Fraud Estimates, 2013-2014, Meet Selected Best Practice Characteristics for Cost Estimation**

Best practice characteristic	Original assessment (2013 <i>Taxonomy</i> )	Updated assessment (2014 <i>Taxonomy</i> )
Provides evidence that the cost estimate was reviewed and accepted by management	Documentation did not provide evidence of management review or approval. However, IRS officials stated they were working on a new process to do so. <b>(partially met)</b>	In February 2016, IRS provided documentation that management reviewed and approved of the 2014 <i>Taxonomy</i> estimates and the new methodology for calculating the refunds paid estimates. <b>(met)</b>
Includes all relevant costs	Estimates included additional categories of IDT returns compared to 2012 estimates, though IRS was unable to estimate the amount of IDT refund fraud associated with undetected schemes due to resource constraints and concerns regarding taxpayer burden. <b>(partially met)</b>	IRS increased the precision of 2014 estimates of IDT paid by using the modeling data set, a new source of individual return-level data. This new methodology incorporates previously undetected schemes in its potential IDT refund fraud population. However, IRS's new methodology omits returns with refund amounts beyond specific thresholds from its fraud estimates for some IDT refunds paid. <b>(partially met)</b>

<sup>48</sup>We did not replicate IRS's *Taxonomy* estimates using tax return data; rather, we reviewed IRS's methodology for calculating the estimates.

<sup>49</sup>IRS developed these guidelines pursuant to the Treasury and General Government Appropriations Act for Fiscal Year 2001 (P.L. 106-554, § 515). OMB, *Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies*, (Washington, D.C.: October 2001), accessed Sept. 24, 2016, [http://www.whitehouse.gov/omb/fedreg\\_final\\_information\\_quality\\_guidelines](http://www.whitehouse.gov/omb/fedreg_final_information_quality_guidelines).

Best practice characteristic	Original assessment (2013 <i>Taxonomy</i> )	Updated assessment (2014 <i>Taxonomy</i> )
Documents all cost-influencing ground rules and assumptions	The <i>Taxonomy</i> documentation noted the assumptions used to develop the estimates but did not provide rationales or analyses to support those assumptions. <b>(partially met)</b>	<i>Taxonomy</i> documentation notes most, but not all assumptions. For example, it does not note that returns resulting in paid refunds were excluded because they were outside thresholds. In addition, the rationales supporting some assumptions, such as the estimated refund values associated with e-file reject returns, were not documented. The assumptions likely result in overestimates for some categories and underestimates for others. <b>(partially met)</b>
Includes a sensitivity analysis <sup>a</sup>	While IRS conducted a sensitivity analysis for one part of the <i>Taxonomy</i> , it did not conduct sensitivity analyses for other categories. <b>(minimally met)</b>	IRS no longer includes a sensitivity analysis for any part of the <i>Taxonomy</i> . In February 2016, IRS officials told us they plan to conduct a sensitivity analysis for assumptions used to calculate <i>Taxonomy</i> estimates. <b>(not met)</b>
Includes a risk and uncertainty analysis <sup>b</sup>	The <i>Taxonomy</i> acknowledges that there is uncertainty in the estimates. However, because of methodology and resource constraints, IRS did not conduct a risk and uncertainty analysis. <b>(minimally met)</b>	IRS does not conduct cost risk and uncertainty analysis for its refunds-prevented estimates. It does present estimates for refunds paid and not recovered as ranges. While these ranges account for risk surrounding known IDT returns that were paid to actual fraudsters, these ranges do not take into account the cumulative impact of additional assumptions. For example, IRS's analysis does not account for the impact of omitting returns that did not meet thresholds. In February 2016, IRS officials told us that they plan to conduct a risk and uncertainty analysis for the <i>Taxonomy</i> . <b>(minimally met)</b>
Results are not overly conservative or optimistic, and are based on most likely costs	Because IRS did not conduct a risk and uncertainty analysis, the level of uncertainty associated with the estimates was unclear. Presenting the <i>Taxonomy</i> as a point estimate did not reflect the inherent uncertainty of the estimate. <b>(minimally met)</b>	IRS made efforts to base refunds paid estimates on a new, more accurate data source and sampling effort. IRS also presented these estimates as ranges that better reflect the inherent uncertainty of the estimates. However, IRS cannot determine the extent to which estimates may be overly conservative or optimistic until it conducts risk and uncertainty analyses. <b>(minimally met)</b>

Source: GAO analysis of IRS *Identity Theft Taxonomy* documentation, GAO-09-3SP, and interviews with IRS officials. | GAO-16-508

Note: We reviewed the *Taxonomy*'s methodology and estimates and evaluated them against selected best practices in the *GAO Cost Guide* that were applicable to the *Taxonomy* and consistent with IRS and OMB information quality guidelines. We focused our analysis on those best practices that we assessed as "partially met" or less in our review of the 2013 *Taxonomy*. See appendix I for an explanation of the methodology we used to determine the ratings.

<sup>a</sup>A sensitivity analysis (also known as "what if" analysis) examines the effect changing assumptions has on the estimate by changing one assumption at a time. It involves recalculating the estimate using differing assumptions to develop ranges of potential estimates.

<sup>b</sup>Risk and uncertainty analysis recognizes the potential for error and captures the cumulative effect that assumptions have on the cost estimate. It involves using methods to develop a range of costs around a point estimate.

As noted in table 1 above, IRS improved the *Taxonomy* to meet one of the best practice characteristics—management review. By reviewing and approving the 2014 *Taxonomy* estimates and the new methodology, IRS management completed a vital step in verifying how estimates were

---

developed. This step helps ensure that management understands the estimate's underlying risks, data sources, and methods so that they are confident that the estimates are accurate, complete, and high in quality.

In the following sections, we analyze in greater detail IRS's efforts to meet best practices outlined in table 1 as well as *Taxonomy* estimates' remaining limitations.

---

### Despite Improvements, Key Weaknesses Affect the Estimate's Accuracy

IRS adopted a new methodology to improve 2014 *Taxonomy* estimates of refunds paid. This new methodology uses the modeling data set, which is based on individual return-level information, to estimate more precisely how much the agency paid to IDT fraudsters. The modeling data set is an improvement over previous data sources that were based on aggregated data. As a result of this improvement, officials can more precisely estimate known IDT refunds paid. Additionally, IRS uses the modeling data set when calculating estimates of likely IDT refunds paid. IRS defines likely IDT returns as returns where the information on the tax return does not match either (1) the current year's information reporting (i.e., information on a W-2); or (2) specific prior-year tax return characteristics.

While the data source used to estimate IDT refunds paid is an improvement from the previous *Taxonomy*, IRS's methodology for calculating estimates for refunds paid excludes select categories of returns that can bias results. A key assumption IRS uses when building its modeling data set for IDT refunds paid is the amount of the refund. As part of its methodology, IRS omits some returns with refund amounts that fail to meet specific refund thresholds from its fraud estimates and does not include all relevant returns in its analysis. IRS officials said IRS uses the thresholds because it wants to prioritize IRS enforcement efforts. In February 2016, IRS officials stated that they did not know how many returns were excluded from the *Taxonomy*. In March 2016, IRS officials said that they are evaluating the extent to which omitted returns met other criteria associated with IRS's definitions of known and likely IDT refund fraud.

According to its *Strategic Plan*, IRS should identify trends, detect high-risk areas of noncompliance, and prioritize enforcement approaches by

---

applying research and advanced analytics.<sup>50</sup> Further, the *GAO Cost Guide* states that analysis should be regularly updated to reflect significant changes in the methodology and should include all relevant costs.<sup>51</sup> While thresholds may help IRS prioritize enforcement efforts on likely IDT fraud schemes, they limit IRS's ability to estimate the entire population of IDT refunds paid. Further, incomplete *Taxonomy* estimates could impede IRS and congressional efforts to assess the effectiveness of its IDT defenses over time. In response to our discussion, IRS officials said that they are considering removing some thresholds and including those returns when calculating estimates of IDT refunds paid for the 2015 *Taxonomy* estimates.

We also found accuracy issues with IRS's estimate of IDT refunds prevented that are likely to result in overestimates. To produce this estimate, IRS uses the *Global Report*, which overestimates the amount of IDT refunds prevented because it overcounts some IDT returns. Overcounting occurs because the *Global Report* aggregates return-level data to create a monthly inventory of confirmed IDT returns. According to IRS officials, the *Global Report* counts each time a return is caught by IRS defenses as a separate instance of refund fraud. For example, if an IDT return is flagged as IDT in both IRS's Electronic Fraud Detection System and its Dependent Database, this return is counted as two IDT returns, even though it is the same return. E-file rejects are also overcounted because a single return can be rejected multiple times.

IRS officials noted that there would be benefits of using return-level data to estimate refunds prevented in the *Taxonomy*, such as avoiding overcounting. However, officials said they use the *Global Report* to develop estimates of prevented IDT refund fraud because it represents IRS's official record of IDT fraud and because IRS has invested substantial resources in improving the report. We agree that the *Global Report* is an important investment for monitoring the effectiveness of IRS's many defenses against fraud, both individually and as a system; however, overcounting the incidence of fraud inflates IRS's *Taxonomy* estimates of the cost of IDT refund fraud, and could potentially bias resource allocation and other decisions. For example, if IRS thinks it is

---

<sup>50</sup>IRS, *Strategic Plan: FY2014-2017*, (Washington, D.C.: June 2014).

<sup>51</sup>[GAO-09-3SP](#).

---

catching 90 percent of estimated IDT refund fraud attempts, agency officials may decide to allocate resources differently than if IRS is, in fact, catching 50 percent.

Our data reliability testing found that the *Global Report's* counts for known IDT returns where IRS prevented the refund were larger than the counts from the modeling data set. Of the estimated \$22.5 billion refunds prevented or recovered in 2014, the *Global Report* included 2.0 million returns worth \$11.4 billion in its known IDT return population, whereas the modeling dataset included 1.6 million returns and \$8.9 billion in its population.<sup>52</sup> Officials acknowledged that they also believe this discrepancy is due to the overcounting in the *Global Report* and could also be caused by the modeling dataset's exclusion of returns that fail to meet specific refund thresholds, as described above.

As noted earlier, IRS's *Strategic Plan* notes that IRS should "identify trends, detect high-risk areas of noncompliance, and prioritize enforcement approaches by applying research and advanced analytics." It also states that IRS should strengthen refund fraud prevention by bolstering analytics capability, making full use of existing data sources, and exploring potential new data sources and techniques.<sup>53</sup> Further, the *GAO Cost Guide* states that estimates be based on primary data sources and contain few mistakes.<sup>54</sup>

By using aggregated data to develop the *Global Report*, the agency's official record of IDT returns is less accurate than if IRS used return-level data. Further, by using the *Global Report* to calculate *Taxonomy* estimates for refunds prevented, IRS may have overestimated the \$22.5 billion in refunds prevented or recovered in the 2014 filing season. As

---

<sup>52</sup>The modeling dataset does not include data on e-file rejects. Therefore, we cannot quantify the extent to which IRS's category 1 estimates of refunds prevented by e-file rejects—worth \$7.3 billion in 2014—are overestimated. IRS officials noted that e-file rejects are the most likely category for overestimating because the same return can be rejected multiple times.

<sup>53</sup>IRS, *Strategic Plan: FY2014-2017* (Washington, D.C.: June 2014).

<sup>54</sup>Primary data are obtained from the original source, can usually be traced to an audited document, are considered the best in quality, and are ultimately the most useful. See [GAO-09-3SP](#) for more details.

described above, inaccurate *Taxonomy* estimates could impede decision makers' ability to monitor the effectiveness of IDT defenses.

**IRS Documents Most Cost Assumptions Used and Plans to Provide Rationales or Analyses to Better Support Assumptions**

In its *Taxonomy* documentation, IRS notes most—but not all—assumptions used to make estimates. For example, IRS does not document that refunds outside of thresholds, as described above, are excluded from IRS's estimates of refunds paid by IRS. In addition, IRS does not always provide rationales or analyses to support the assumptions it does document. For example, IRS does not provide a rationale for the average refund value used to estimate the cost of electronically filed returns that IRS rejects (i.e., e-file rejects) and categorizes as IDT returns, which affects the total value of IRS's refunds prevented estimates.

Our analyses show that using different refund assumptions can affect the refunds prevented estimate by billions of dollars. Because IRS does not have reliable data on the refund values associated with e-file rejects, it uses the average refund value of returns detected by various IDT defenses. As noted in table 2, IRS's estimate assumes the average refund value for all IDT defenses (\$5,959), which results in \$7.3 billion dollars prevented on 1.2 million e-filed returns. However, the average refund value of e-file returns detected by IRS IDT defenses varies—indicating uncertainty in the estimates. For example, if IRS used the different average refunds in table 2 to develop its e-file reject estimate, the total could range from \$4.1 billion to \$7.5 billion.

**Table 2: Potential Estimates of E-file Rejects Using Different IRS Identity Theft (IDT) Defenses, 2014**

<b>IDT defense</b>	<b>Average refund (in dollars per refund)</b>	<b>Number of e-file rejects (in millions)</b>	<b>Total value of refunds prevented by e-file rejects (in billions of dollars)</b>
Unpostable <sup>a</sup>	3,383	1.2M	4.1
Returns detected as part of a repeat "Operation Mass Mail" Scheme <sup>b</sup>	3,943	1.2M	4.8
Fraud filters (Electronic Fraud Detection System)	5,989	1.2M	7.3
IDT filters (Dependent Database)	6,138	1.2M	7.5
IRS estimate using average refund value for all IDT defenses	5,959	1.2M	7.3

Source: GAO Analysis of IRS data | GAO-16-508.

<sup>a</sup>Returns are "unpostable" when they fail to pass validity checks within IRS systems. An account with certain identity theft indicators will cause a return to unpost.

---

<sup>b</sup>IRS defenses search for returns associated with the “Operation Mass Mail” scheme, where identity thieves use the stolen identities of Puerto Rican citizens and individuals from other U.S. territories.

We previously recommended that IRS document the analysis underlying the cost-influencing assumptions.<sup>55</sup> As stated above, IRS officials told us they are working to implement this recommendation by October 2016. Given the evolving nature of IDT refund fraud, documenting *Taxonomy* assumptions and the rationales used to develop those assumptions in accordance with our prior recommendations would enable IRS management and policymakers to determine whether the assumptions remain valid or need to be revised or updated.

---

## IRS Still Faces Challenges in Improving Its Reporting of Risk and Uncertainty

IRS is still working to improve its reporting of the inherent imprecision and uncertainty of its *Taxonomy* estimates. Previously, we found that IRS presented 2013 *Taxonomy* estimates as point estimates, which did not represent the *Taxonomy*'s inherent uncertainty. We recommended that IRS report the inherent imprecision and uncertainty of the estimates and noted that one way IRS could do this would be to present a range of values for its *Taxonomy* estimates.<sup>56</sup> High-quality cost estimates usually fall within a range of possible costs, with the point estimate between the best and worst case extremes. Having a range of costs around a point estimate is more useful to decision makers because it indicates the uncertainty in the estimates by conveying its level of confidence or by conveying the level of confidence of the most likely cost.<sup>57</sup> Knowing the uncertainty related to *Taxonomy* estimates could affect different decisions about how to allocate resources to combat IDT refund fraud. For example, if there is 80 percent confidence in IRS's estimates, then decision makers may make different decisions than if there is 50 percent confidence in the estimates.

Under its revised methodology, IRS partially addressed our previous recommendation by presenting refunds-paid estimates as a range rather than a single point estimate to reflect the uncertainty in IRS's estimate of

---

<sup>55</sup> [GAO-15-119](#), p.26.

<sup>56</sup> [GAO-15-119](#).

<sup>57</sup> In this context, a confidence level is the probability that the true cost is at or below a chosen value out of a certain number of simulations through a risk and uncertainty analysis.

---

the revenue lost to IDT refund fraud. In addition, IRS took steps to incorporate better quality data into its refunds paid estimate by utilizing both the modeling data set's return-level information and results from a new sampling effort. However, these ranges may not give decision makers a truly accurate understanding of what IRS knows and does not know about IDT refund fraud because they are not derived from a cost risk and uncertainty analysis. Such an analysis accounts for the cumulative impact that multiple assumptions might have on IRS's estimates. For example, ranges do not account for uncertainty regarding the extent to which IRS's estimates account for all IDT fraud schemes. Additionally, IRS officials manually review some returns to determine whether or not the returns are IDT or non-IDT returns. IRS's ranges also do not account for the uncertainty or the risk that manual reviewers may not accurately characterize returns as IDT returns and non-IDT returns.

In addition, IRS does not conduct a sensitivity analysis for *Taxonomy* categories that include assumptions. A sensitivity analysis reveals critical assumptions and cost drivers that most affect estimate results, and can help managers take steps to ensure the estimates' quality. By conducting a sensitivity analysis, IRS will know which assumptions and which factors affect the *Taxonomy* the most so IRS can devote resources to combating IDT refund in those areas and work to make the estimates more accurate in those areas.

Until IRS addresses our prior recommendations and provides an indication of uncertainty in the *Taxonomy* estimates, the false sense of precision could affect decisions about how to allocate resources to combat IDT refund fraud. IRS officials told us in February 2016 that they plan to conduct a sensitivity analysis and a risk and uncertainty analysis for the assumptions that are used when IRS calculates the updated *Taxonomy* estimates for 2015.

---

## Conclusions

IRS's continued efforts to improve TPP are critical to combatting IDT refund fraud. Though IRS has made improvements to TPP, evidence suggests that the agency's efforts to authenticate taxpayers in filing season 2015 may not have kept pace with the evolving threat of IDT refund fraud. Since IRS last conducted a risk assessment for TPP, PII has become more widely disseminated, and IRS has changed TPP procedures. In addition, though IRS is undertaking efforts to strengthen Get Transcript, a program that poses risks similar to TPP, IRS has not determined whether authentication improvements are necessary for TPP. Documenting time frames and conducting an updated e-authentication

---

risk assessment for TPP's remote authentication options would enable IRS to identify opportunities and take actions to strengthen TPP authentication in accordance with appropriate standards. In turn, strengthened authentication would help IRS reduce revenue lost to IDT fraudsters, improve the efficiency of fraud filter investments, and reduce the number of legitimate taxpayers who become victims of IDT refund fraud.

IRS's monitoring of the extent of IDT refund fraud is key to supporting decision makers' ability to determine how to combat IDT refund fraud. IRS has invested a considerable effort in monitoring and reporting the extent of IDT refund fraud through its *Taxonomy* estimates. However, the accuracy of IRS's IDT refund fraud reporting in the *Taxonomy* estimates could be improved. For example, using return-level data, such as the modeling data set, could improve the accuracy of the *Taxonomy*'s refunds paid estimates. More accurate *Taxonomy* estimates would help IRS better understand how and to what extent IDT refund fraud is evading IRS defenses. This would allow it to focus attention on where the risk is greatest and improve the design of its IDT filters. Additionally, reducing overcounting and ensuring all relevant IDT returns—even those that fail to meet specific refund thresholds—are included in *Taxonomy* estimates could help IRS communicate more accurate information on the amount and cost of IDT refund fraud to decision makers. Finally, implementing our past recommendations will help IRS further improve the reliability of its estimates.

---

## Recommendations

To further deter noncompliance in the Taxpayer Protection Program, we recommend that the Commissioner of Internal Revenue take the following two actions in accordance with OMB and NIST e-authentication guidance:

1. conduct an updated risk assessment to identify new or ongoing risks for TPP's online and phone authentication options, including documentation of time frames for conducting the assessment, and
2. implement appropriate actions to mitigate risks identified in the assessment.

To improve the quality of the *Taxonomy*'s IDT refund fraud estimates, we recommend that the Commissioner of Internal Revenue take the following two actions:

1. remove refund thresholds from criteria used to develop IRS's refunds-paid estimates, and

- 
2. utilize return-level data—where available—to reduce overcounting and improve the quality and accuracy of the refunds-prevented estimates.

---

## Agency Comments and Our Evaluation

We provided a draft of this product to the Commissioner of Internal Revenue, the Attorney General, and the Director of the Federal Bureau of Investigation for review and comment. In its written comments, reproduced in appendix III, IRS agreed with our TPP recommendations and neither agreed nor disagreed with our *Taxonomy* recommendations.

IRS stated that it will conduct an updated risk assessment for TPP's online electronic authentication application, in accordance with OMB and NIST guidelines. Regarding TPP's phone authentication option, IRS reported that a portion of the telephone authentication option will be included in the assessment because IRS employees use a web interface. As noted in the report, we believe that following a consistent authentication standard for both online and phone authentication would help prevent IDT fraudsters from shifting authentication attempts to the option that requires a less rigorous standard. IRS officials stated that they will implement mitigation actions identified during the assessment, to the degree feasible. We continue to emphasize the importance of implementing appropriate actions to mitigate identified risks because doing so would improve TPP authentication and prevent additional fraudulent refunds from being issued.

Consistent with our recommendation, IRS stated that it has reduced the lower threshold used to develop its IDT refund-paid estimate in its 2014 modeling dataset. IRS did not change its upper threshold. IRS also stated that the risk of this remaining threshold excluding relevant IDT returns is mitigated because IRS manually reviews such returns. We support IRS's reduction of the lower threshold and its manual review of high-value refunds.

With regard to our recommendation to use return-level data to reduce overcounting and improve the accuracy of the refunds-prevented estimate, IRS officials said that they are discussing the impact of the recommendation and determining if it is feasible to implement. As previously noted, it is important for IRS to provide accurate estimates of the IDT fraud it prevented or recovered. By not using return-level data, the *Global Report* overcounts some IDT returns. As a result, IRS is providing Congress and other stakeholders with overestimates of the amount of IDT refund fraud it prevented or recovered.

---

The Department of Justice provided technical comments for itself and the Federal Bureau of Investigation, which we incorporated as appropriate.

---

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to the Commissioner of Internal Revenue, the Attorney General of the United States, and the Director of the Federal Bureau of Investigation. In addition, the report will be available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at (202) 512-9110 or [mctiguej@gao.gov](mailto:mctiguej@gao.gov). Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix IV.



James R. McTigue, Jr.  
Director, Tax Issues  
Strategic Issues

---

# Appendix I: Objectives, Scope, and Methodology

---

This report (1) evaluates the performance of Internal Revenue Service's (IRS) Taxpayer Protection Program (TPP) and (2) assesses IRS efforts to improve its estimates of identity theft (IDT) refund fraud costs for 2014. The report discusses IDT refund fraud and not employment fraud.<sup>1</sup> Detailed information on IRS's enforcement efforts was excluded from the report because of sensitivity concerns.

To evaluate TPP's performance, we reviewed IRS studies designed to identify and support ongoing identity authentication refinements to TPP.<sup>2</sup> We compared specifics of IRS's TPP against relevant guidance on enterprise risk management, electronic authentication, and internal controls.<sup>3</sup> We assessed IRS's TPP analysis by (1) reviewing relevant IRS documentation, (2) conducting manual testing to identify obvious errors, and (3) interviewing IRS officials.

During the course of our work, we found that IRS likely underestimated the value of refunds issued to IDT fraudsters in filing season 2015 via TPP because the agency did not account for all refunds potentially paid to IDT refund fraudsters who passed TPP authentication. To assess how excluding potential IDT refunds affected IRS's estimates of the amount potentially paid to IDT fraudsters who were able to pass TPP authentication, we conducted a scenario analysis. We chose not to base our scenarios on IRS's past research because it used a nongeneralizable sample and because its methodology for identifying close matches changed from 2014 to 2015.<sup>4</sup> Instead, we identified scenarios of 5 to 10

---

<sup>1</sup>IDT employment fraud occurs when a fraudster uses a taxpayer's name and Social Security number to obtain a job.

<sup>2</sup>IRS Office of Compliance Analytics, *IRS Response to GAO TPP Questions*, (Dec. 16, 2015); *Taxpayer Protection Program Identity Authentication Analytics Update*, (Mar. 23, 2015); *Taxpayer Protection Program Authentication Analysis Summary from Year 2014*, (February 2015); and *TPP Authentication Analytics Executive Update* (Feb. 18, 2015).

<sup>3</sup>IRS, *Internal Revenue Service Enterprise Risk Management Program: Concept of Operations*, (Washington, D.C., May 18, 2015); National Institute of Standards and Technology, *Electronic Authentication Guideline*, Special Publication 800-63-2, (August 2013); Office of Management and Budget, *E-Authentication Guidance for Federal Agencies*, M-04-04 (Washington, D.C.: Dec. 16, 2003); and GAO, *Standards for Internal Control in the Federal Government*, [GAO/AIMD-00-21.3.1](#) (Washington, D.C.: Nov. 1, 1999).

<sup>4</sup>IRS, *Taxpayer Protection Program Authentication Analysis Summary from Year 2014* (February 2015).

---

percent to illustrate the potential outcomes if relatively small percentages of these returns were actually IDT.

To assess IRS's efforts to improve its *Identity Theft Taxonomy (Taxonomy)* estimates of IDT refund fraud for 2014, we reviewed the *Taxonomy's* methodology and estimates. We then evaluated them against selected best practices in the *GAO Cost Estimating and Assessment Guide (GAO Cost Guide)* that were applicable to the *Taxonomy* and consistent with IRS and Office of Management and Budget (OMB) information quality guidelines.<sup>5</sup> These best practices are relevant because the *Taxonomy* is an estimate of the amount of revenue lost to IDT refund fraud—a cost to taxpayers. To develop this guide, our cost experts assessed the measures consistently applied by cost-estimating organizations throughout the federal government and industry; based upon this assessment, the cost experts then considered best practices for the development of reliable cost estimates. We focused our analysis on those best practices that we assessed as “partially met” or less in our review of the 2013 *Taxonomy* (see text box).<sup>6</sup> In comparing 2014 estimates with 2013 estimates, we could not determine if differences in *Taxonomy* estimates between these years were due to changes in methodology, IDT fraud trends, or the efficacy of IRS's IDT defenses. During our review of the 2013 *Taxonomy*, we discussed the *GAO Cost Guide's* best practices with IRS officials who generally agreed with their applicability to the *Taxonomy*.

---

<sup>5</sup>GAO, *GAO Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs*, [GAO-09-3SP](#) (Washington, D.C.: March 2009) and Office of Management and Budget, *Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies* (Washington, D.C.: October 2001), accessed Feb. 11, 2016, [https://www.whitehouse.gov/omb/fedreg\\_final\\_information\\_quality\\_guidelines/](https://www.whitehouse.gov/omb/fedreg_final_information_quality_guidelines/). IRS developed information quality guidelines to ensure that information the agency reports is objective. Objectivity, as defined in OMB quality guidelines, involves ensuring information is reliable, accurate, and unbiased. Objectivity also involves presenting information in a clear, complete, and unbiased manner.

<sup>6</sup>[GAO-15-119](#).

**Best Practices in Cost Estimating Used to Review the 2014 *Taxonomy***

We assessed the *Taxonomy* against the following best practices for objective, reliable cost estimates:

- Include all relevant costs.
- Document all cost-influencing ground rules and assumptions.
- Include a sensitivity analysis.
- Include a risk and uncertainty analysis.
- Are not overly conservative or optimistic, and are based on most likely costs.
- Provide evidence that the cost estimate was reviewed and accepted by management.

Source: GAO. | GAO-16-508

To analyze IRS's *Taxonomy* against the best practices, we reviewed *Taxonomy* documentation, conducted manual and electronic data testing, reviewed coding for obvious errors, compared underlying data to IRS's *Refund Fraud & Identity Theft Global Report*, and interviewed IRS officials to understand the methodology used to create the 2014 estimates and how that methodology changed from that used to develop the 2013 *Taxonomy*. We did not replicate IRS's *Taxonomy* estimates using tax return data; rather, our focus was on IRS's methodology for calculating the estimates. We developed an overall assessment rating for each best practice using the following definitions:

- **Not met.** IRS provided no evidence that satisfied any portion of the best practice.
- **Minimally met.** IRS provided evidence that satisfied a small portion of the best practice.
- **Partially met.** IRS provided evidence that satisfied about half of the best practice.
- **Substantially met.** IRS provided evidence that satisfies a large portion of the best practice.
- **Met.** IRS provided complete evidence that satisfies the entire best practice.

We conducted this performance audit from March 2015 to May 2016 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

# Appendix II: Status of Our Prior Identity Theft Refund Fraud Recommendations

This report is the third in a series of our reports on identity theft (IDT) refund fraud. Since August 2014, we have issued two reports that included eight recommendations on actions the Internal Revenue Service (IRS) can take to monitor and combat IDT refund fraud. As of March 2016, IRS implemented three of the eight recommendations, and it is implementing the remaining five recommendations. Table 3 summarizes our prior recommendations and their implementation status.

**Table 3: Prior GAO Recommendations to IRS Related to Identity Theft (IDT) Refund Fraud**

Recommendation	Benefit	Status
<p><a href="#">GAO-14-633</a> – We recommended that the Commissioner of Internal Revenue should</p>	<p>Earlier access to W-2s could help IRS match W-2 information to taxpayers' returns and identify discrepancies before issuing billions of dollars of fraudulent IDT refunds. How IRS implements W-2 matching could affect the costs and benefits for itself and other stakeholders (e.g., logistical challenges for the Social Security Administration, which processes W-2 data before transmitting them to IRS).</p>	<p><b>Implemented.</b> In September 2015, IRS provided us with a document detailing the costs and benefits of W-2 acceleration. The document discussed the IRS systems and work processes that will need to be adjusted to accommodate earlier, prerefund matching of W-2s; the time frames for when these changes could be made; potential impacts on taxpayers, IRS, and other parties; and what other changes will be needed (such as delaying refunds) to ensure IRS can match tax returns to W-2 data before issuing refunds.<sup>a</sup></p>
<p>fully assess the costs and benefits of accelerating W-2 deadlines and provide information to Congress on potential impacts on taxpayers, IRS, the Social Security Administration, and third parties.</p>	<p>See description of benefits above.</p>	<p><b>Implemented.</b> See description above.</p>
<p>fully assess the costs and benefits of accelerating W-2 deadlines and provide information to Congress on what other changes will be needed (such as delaying the start of the filing season or delaying refunds) to ensure IRS can match tax returns to W-2 data before issuing refunds.</p>	<p>See description of benefits above.</p>	<p><b>Implemented.</b> See description above.</p>

**Appendix II: Status of Our Prior Identity Theft  
Refund Fraud Recommendations**

<p>provide aggregated information on (1) the success of external party leads in identifying suspicious returns and (2) emerging trends (pursuant to section 6103 restrictions).</p>	<p>This feedback would help financial institutions know if the leads they provide to IRS are useful and would help them improve their own detection tools.</p>	<p><b>Implementation in progress.</b> In November 2014, IRS reported that it would implement our recommendation by November 2015. In November 2015, IRS reported that it had developed a database to track leads submitted by financial institutions and the results of those leads. IRS also stated that it had held two sessions with financial institutions to provide feedback on external leads provided to IRS. In December 2015, IRS officials stated that the agency had sent a customer satisfaction survey asking financial institutions for feedback on the external leads process and was considering other ways to provide feedback to financial institutions. However, to date IRS has not provided feedback to the majority of relevant lead-generating third parties.</p>	
<p>develop a set of metrics to track external leads by the submitting third party.</p>	<p>This feedback would help financial institutions know if the leads they provide to IRS are useful and would help them improve their own detection tools.</p>	<p><b>Implementation in progress.</b> See description above.</p>	
<p><b>GAO-15-119</b> – We recommended that the Commissioner of Internal Revenue should</p>	<p>follow relevant best practices outlined in GAO's <i>Cost Assessment Guide: Best Practices for Estimating and Managing Program Costs (GAO Cost Guide)</i> by documenting the underlying analysis justifying cost-influencing assumptions.</p>	<p>Given the evolving nature of IDT refund fraud, documenting the rationales for assumptions would help IRS management and policymakers determine whether the assumptions remain valid or need to be updated.</p>	<p><b>Implementation in progress.</b> In April 2015, IRS reported that it would implement our recommendation by mid-October 2016. In October 2015, IRS provided updated <i>Taxonomy</i> estimates for 2014. This new analysis and documentation noted most but not all assumptions. For example, it did not note that some returns resulting in paid refunds were excluded because they were outside thresholds. In addition, the rationales supporting some assumptions, such as the estimated refund values associated with e-file reject returns, were not documented.</p>

---

---

follow relevant best practices outlined in the *GAO Cost Guide* by reporting the inherent imprecision and uncertainty of the estimates. For example, IRS could provide a range of values for its *Taxonomy* estimates.

Reporting the uncertainty that is already known from IRS analysis (and conducting further analyses when not cost prohibitive) might help IRS communicate IDT refund fraud's inherent complexity. While a point estimate might lead to one decision, a range that reflects the uncertainty may lead decision makers to a different decision.

**Implementation in progress.** In April 2015, IRS reported that it would implement this recommendation by mid-October 2016. In September 2015, IRS provided updated *Taxonomy* estimates for 2014 that presented the estimates for refunds paid and not recovered as ranges. While these ranges account for risk surrounding known IDT returns that were paid to actual fraudsters, these ranges do not take into account the cumulative impact of additional assumptions on the estimate. For example, IRS's analysis does not account for the impact of how IRS defines the population of likely IDT returns. IRS should conduct additional analyses to understand the estimates' uncertainty and report the imprecision and uncertainty of the estimates. Specifically, sensitivity analysis could help IRS understand how each assumption affects the estimates.<sup>b</sup> A risk and uncertainty analysis could help IRS understand the cumulative impact of all assumptions on the *Taxonomy* estimates.<sup>c</sup>

---

should estimate and document the costs, benefits and risks of possible options for taxpayer authentication, in accordance with Office of Management and Budget and National Institute of Standards and Technology guidance.

Analysis of costs, benefits, and risks could help inform IRS's and Congress's decisions about whether and how much to invest in the various authentication options.

**Implementation in progress.** In April 2015, IRS reported that it would implement our recommendation by November 2015. In late 2015, IRS officials told us that the agency has developed guidance for the authentication group to assess costs, benefits, and risks, and that its analysis will inform decision making on authentication-related issues.<sup>d</sup> While IRS is making progress, it has yet to analyze the costs, benefits, and risks of the range of authentication options available and has not used analysis to select which authentication options to use for specific types of taxpayer interactions. We continue to monitor IRS's progress.

Source: GAO and IRS. | GAO-16-508.

<sup>a</sup>In December 2015, the Consolidated Appropriations Act, 2016, amended the tax code to accelerate W-2 filing deadlines to January 31. This change goes into effect for W-2s reporting payments made in 2016 and filed in 2017. Pub. L. No. 114-113, div. Q, § 201, 129 Stat. 2242 (Dec. 18, 2015).

<sup>b</sup>A sensitivity analysis (also known as what if analysis) examines the effect changing assumptions has on an estimate by changing one assumption at a time. It involves recalculating the estimate using differing assumptions to develop ranges of potential estimates.

<sup>c</sup>Risk and uncertainty analysis recognizes the potential for error and captures the cumulative effect that assumptions have on the cost estimate. It involves using methods to develop a range of costs around a point estimate.

<sup>d</sup>The authentication group later became the Identity Assurance Office.

In addition to these eight recommendations, we also identified a matter for congressional consideration to help IRS combat IDT refund fraud. In August 2014, we reported that Congress should consider providing the Secretary of the Treasury with the regulatory authority to lower the threshold for electronic filing of the W-2, from 250 returns annually to between 5 to 10 returns, as appropriate. As discussed in table 3 above, earlier access to W-2s could help IRS match W-2 information to taxpayers' returns and identify discrepancies before issuing billions of dollars of fraudulent IDT refunds. However, paper W-2s are unavailable for IRS matching until later in the year due to the additional time needed to process paper forms. The Social Security Administration estimated that

to meaningfully increase the electronic filing (e-filing) of W-2s, the threshold would have to be lowered to include those filing 5 to 10 W-2s.<sup>1</sup> In addition, the Social Security Administration estimated an administrative cost savings of about 50 cents per e-filed W-2. Based on these cost savings and the ancillary benefits they provide in supporting IRS's efforts to conduct more prerefund matching, a change in the e-filing threshold is warranted. As of March 2016, Congress has not acted on this matter for consideration.

---

<sup>1</sup>According to Social Security Administration officials, the agency would be able to easily process W-2s regardless of the threshold requirement for electronic filing of W-2s.

# Appendix III: Comments from the Internal Revenue Service



DEPUTY COMMISSIONER

DEPARTMENT OF THE TREASURY  
INTERNAL REVENUE SERVICE  
WASHINGTON, D.C. 20224

May 9, 2016

Mr. James R. McTigue  
Director, Tax Issues  
U.S. Government Accountability Office  
441 G Street, N.W.  
Washington, DC 20548

Dear Mr. McTigue:

I have reviewed the draft report entitled *IDENTITY THEFT AND TAX FRAUD: IRS Needs to Update Risk Assessment for the Taxpayer Protection Program*, and appreciate your acknowledgment of the actions we have taken to address identity theft (IDT) and tax fraud through increased focus in our strategic planning and significant resources devoted to address this issue. I also appreciate your acknowledgment of the various tools and programs that we have developed, including the use of automated IDT filters to identify suspicious returns during processing, the Taxpayer Protection Program (TPP) to assist in authenticating taxpayer identities, issuance of Identity Protection Personal Identification Numbers to protect IDT victims, and development of the Security Summit group.

Securing our systems and taxpayer data continues to be a top priority for the IRS. We continue to devote significant time and attention to this challenge, despite constrained resources as a result of repeatedly decreased funding over the past few years. Because IDT criminals have significant resources to devote to their schemes, their methods are constantly evolving. As such, we continually analyze and look for ways to improve IDT detection, and make any necessary adjustments to our filters and processes. We are finding that tax-related IDT schemes are growing at an alarming rate with increasing complexity and sophistication. Perpetrators are no longer just individual criminals with a personal laptop and a list of stolen social security numbers and prepaid cards. Instead, these criminals are part of organized internet crime syndicates who are networked across the world and have turned IDT and tax fraud into a highly lucrative business, with deep resources to avoid detection.

Recognizing that a single effort will not deter or improve IDT trends, the IRS is leading multiple initiatives to address this growing threat. Realizing we are only one stakeholder in the battle against IDT, we're working with our partners through the Security Summit group to identify additional opportunities to address IDT refund fraud. This

unprecedented group is the first public-private partnership of its kind with the goal of putting new and innovative safeguards in place to protect taxpayers. By working together, the IRS, state tax administrators, and private-sector tax industry leaders will help protect taxpayers' information and the integrity of the federal and state tax systems.

The Security Summit group has made progress on a number of initiatives this past year. During the 2016 filing season, Security Summit partners have helped the IRS improve its ability to spot potentially false returns before they are processed and thus before a possibly fraudulent refund is issued. Under our industry leads program, Security Summit partners and other external stakeholders such as banks provide information that allows us to improve our fraud filters, which in turn leads to more suspicious returns suspended for further review.

Significant steps are taken to authenticate the taxpayer when our filters identify potential risk for IDT or fraud. The TPP was implemented to identify and treat potential IDT and non-compliant returns based on a series of models, filters, and business rules, and increase revenue protection by applying filters to existing business rules in order to identify IDT and non-compliant returns in a pre-refund environment, while providing refunds to compliant taxpayers in a timely manner. It allows us to explore past trends or schemes to determine common characteristics of IDT, or non-compliant returns and use these characteristics to create new models, filters, and business rules. For example, this filing season we implemented the use of specific filters to address emerging fraud, such as Get Transcript data breaches. This provided us with an enhanced opportunity to review returns that were potentially impacted by this heightened level of risk. We worked diligently to move good taxpayers through our processes to prevent excessive delays in refunds by shortening some internal procedural timeframes and improving level of service.

We have also increased our efforts to authenticate or validate third party data by implementing an Accelerated W-2 process this filing season. As of February 17, 2016, the IRS had received nearly 26 million early W-2s directly from certain reporting agents, Federal agencies, and employers. In addition to W-2s the IRS received directly during the 2016 filing season, the IRS provided outreach to various reporting agents requesting that W-2s be filed with the Social Security Administration (SSA) earlier in the year. Based on this effort, the IRS has processed, in the Information Return Masterfile, approximately 78 million W-2s received from SSA by February 17, 2016. This is approximately 33 percent of the total Tax Year (TY) 2015 W-2s that the IRS expects to process for TY 2015. At this point last year, the IRS had only processed 9 percent of all TY 2014 W-2s. Having W-2s earlier will make it easier for the IRS to verify the legitimacy of tax returns at the point of filing and to spot fraudulent returns.

The Taxonomy methodologies and IDT protection strategies are reviewed annually to make necessary improvements for upcoming filing seasons. As noted in the report, due to the challenges inherent in estimating fraudulent activity and the evolving nature of

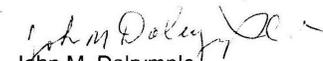
3

fraud schemes, our efforts to improve the Taxonomy estimates will likely be an ongoing process.

We realize more work needs to be done regarding taxpayer authentication and agree an updated risk assessment should be conducted for the TPP. As the IRS enhances return processing filters and catches more fraudulent returns at the time of filing, criminals have become more sophisticated at faking taxpayers' identities so they can evade those filters and successfully obtain fraudulent refunds. A key element in our efforts to improve protections for existing online tools and future ones is the development of a strong, coordinated, and evolving authentication framework. This framework will enable us to require multifactor authentication for all online tools and applications that warrant a high level of assurance. The IRS recently created a new position, the IRS Identity Assurance Executive, to lead in the development of our service-wide approach to authentication. We have also engaged with the U.S. Digital Service, which uses the best of product design, engineering practices, and technology professionals to build effective, efficient, and secure digital channels to transform the way government works for taxpayers.

Responses to your specific recommendations are enclosed. If you have any questions, please contact Ken Corbin, Director, Return Integrity and Compliance Services, Wage and Investment Division, at (404) 338-9042.

Sincerely,

  
John M. Dalrymple  
Deputy Commissioner for  
Services and Enforcement

Enclosure

Enclosure

**Recommendations**

**RECOMMENDATION 1**

To further deter noncompliance in the Taxpayer Protection Program, we recommend that the Commissioner of Internal Revenue take the following two actions, in accordance with OMB and NIST e-authentication guidance:

- Conduct an updated risk assessment to identify new or ongoing risks for TPP's online and phone authentication options, including documentation of timeframes for conducting the assessment, and
- Implement appropriate actions to mitigate risks identified in the assessment.

**COMMENT**

The IRS will conduct an updated e-authentication risk assessment for the Taxpayer Protection Program's (TPP) online e-authentication application. As it has in the past, the IRS will follow OMB M-04-04 and NIST 800-63 R2 guidelines when conducting the TPP e-authentication risk assessment to determine an assurance level commensurate with sensitivity of data or transaction type for web applications. To the extent that TPP-assigned contact representatives continue to use a web interface, that portion of telephonic contact will also be included in the e-authentication risk assessment.

**RECOMMENDATION 2**

To improve the quality of the *Taxonomy's* IDT refund fraud estimates, we recommend that the Commissioner of Internal Revenue take the following two actions:

- Remove refund thresholds from criteria used to develop IRS's refunds-paid estimates, and
- Utilize return-level data, where available, in order to reduce overcounting and improve the quality and accuracy of the refunds-prevented estimates.

**COMMENT**

The IRS reduced one of two thresholds (Lower Limit) for IDT 1, 2, and 3 in the Tax Year 2014 modeling dataset. This, in turn, will result in the reporting of additional returns outside current thresholds. The risk in the remaining threshold is mitigated because the IRS manually reviews returns outside of the remaining threshold (Upper Limit).

Return-level data and the IDT Global Report are not mutually exclusive. The Global Report does use estimates from return-level data to provide values for the Confirmed Refund Protected Dashboard section of the Global Report (among other sections). The IDT Taxonomy uses the Global IDT Report because it is the report used by IRS leadership to see the impact of counter-IDT efforts (on a monthly basis). Since we

2

began the IDT mission, the IRS has continually improved its tracking of IDT, which is reflected in the Global IDT report.

---

# Appendix IV: GAO Contact and Staff Acknowledgments

---

## GAO Contact

James R. McTigue, Jr., (202) 512-9110 or [mctiguej@gov](mailto:mctiguej@gov).

---

## Staff Acknowledgments

In addition to the individual named above, Neil Pinney, Assistant Director; Shannon Finnegan, Analyst-in-Charge; Lisette Baylor; Dawn Bidne; Amy Bowser; Sara Daleski; Deirdre Duffy; Michele Fejfar; Lauren Friedman; Robert Gebhart; Jason Lee; Dae Park; Jeffrey Daniel Paulk; Robert Robinson; and Albert Sim made key contributions to this report. Joanna Berry, Gary Bianchi, Mark Canter, Nina Crocker, Jeffrey Knott, Paul Middleton, Sabine Paul, Sara Pelton, Bradley Roach, and Julie Spetz also provided assistance.

---

# Appendix V: Accessible Data

---

## Agency Comment Letter

---

Text of Appendix III:  
Comments from the  
Internal Revenue Service

---

Page 1

DEPARTMENT OF THE TREASURY

INTERNAL REVENUE SERVICE

WASHINGTON, D.C. 20224

DEPUTY COMMISSIONER

May 9, 2016

Mr. James R. McTigue

Director, Tax Issues

U.S. Government Accountability Office

441 G Street, N.W.

Washington, DC 20548

Dear Mr. McTigue:

I have reviewed the draft report entitled IDENTITY THEFT AND TAX FRAUD: IRS Needs to Update Risk Assessment for the Taxpayer Protection Program, and appreciate your acknowledgment of the actions we have taken to address identity theft (IDT) and tax fraud through increased focus in our strategic planning and significant resources devoted to address this issue. I also appreciate your acknowledgment of the various tools and programs that we have developed, including the use of automated IDT filters to identify suspicious returns during processing, the Taxpayer Protection Program (TPP) to assist in authenticating taxpayer identities, issuance of Identity Protection Personal Identification

Numbers to protect IDT victims, and development of the Security Summit group.

Securing our systems and taxpayer data continues to be a top priority for the IRS. We continue to devote significant time and attention to this challenge, despite constrained resources as a result of repeatedly decreased funding over the past few years. Because IDT criminals have significant resources to devote to their schemes, their methods are constantly evolving. As such, we continually analyze and look for ways to improve IDT detection, and make any necessary adjustments to our filters and processes. We are finding that tax-related IDT schemes are growing at an alarming rate with increasing complexity and sophistication. Perpetrators are no longer just individual criminals with a personal laptop and a list of stolen social security numbers and prepaid cards. Instead, these criminals are part of organized internet crime syndicates who are networked across the world and have turned IDT and tax fraud into a highly lucrative business, with deep resources to avoid detection.

Recognizing that a single effort will not deter or improve IDT trends, the IRS is leading multiple initiatives to address this growing threat. Realizing we are only one stakeholder in the battle against IDT, we're working with our partners through the Security Summit group to identify additional opportunities to address IDT refund fraud. This

---

Page 2

unprecedented group is the first public-private partnership of its kind with the goal of putting new and innovative safeguards in place to protect taxpayers. By working together, the IRS, state tax administrators, and private-sector tax industry leaders will help protect taxpayers' information and the integrity of the federal and state tax systems.

The Security Summit group has made progress on a number of initiatives this past year. During the 2016 filing season, Security Summit partners have helped the IRS improve its ability to spot potentially false returns before they are processed and thus before a possibly fraudulent refund is issued. Under our industry leads program, Security Summit partners and other external stakeholders such as banks provide information that allows us to improve our fraud filters, which in turn leads to more suspicious returns suspended for further review.

Significant steps are taken to authenticate the taxpayer when our filters identify potential risk for IDT or fraud. The TPP was implemented to identify and treat potential IDT and non-compliant returns based on a series of models, filters, and business rules, and increase revenue

protection by applying filters to existing business rules in order to identify IDT and non-compliant returns in a pre-refund environment, while providing refunds to compliant taxpayers in a timely manner. It allows us to explore past trends or schemes to determine common characteristics of IDT, or non-compliant returns and use these characteristics to create new models, filters, and business rules. For example, this filing season we implemented the use of specific filters to address emerging fraud, such as Get Transcript data breaches. This provided us with an enhanced opportunity to review returns that were potentially impacted by this heightened level of risk. We worked diligently to move good taxpayers through our processes to prevent excessive delays in refunds by shortening some internal procedural timeframes and improving level of service.

We have also increased our efforts to authenticate or validate third party data by implementing an Accelerated W-2 process this filing season. As of February 17, 2016, the IRS had received nearly 26 million early W-2s directly from certain reporting agents, Federal agencies, and employers. In addition to W-2s the IRS received directly during the 2016 filing season, the IRS provided outreach to various reporting agents requesting that W-2s be filed with the Social Security Administration (SSA) earlier in the year. Based on this effort, the IRS has processed, in the Information Return Masterfile, approximately 78 million W-2s received from SSA by February 17, 2016. This is approximately 33 percent of the total Tax Year (TY) 2015 W-2s that the IRS expects to process for TY 2015. At this point last year, the IRS had only processed 9 percent of all TY 2014 W-2s. Having W-2s earlier will make it easier for the IRS to verify the legitimacy of tax returns at the point of filing and to spot fraudulent returns.

The Taxonomy methodologies and IDT protection strategies are reviewed annually to make necessary improvements for upcoming filing seasons. As noted in the report, due to the challenges inherent in estimating fraudulent activity and the evolving nature of

---

Page 3

fraud schemes, our efforts to improve the Taxonomy estimates will likely be an ongoing process.

We realize more work needs to be done regarding taxpayer authentication and agree an updated risk assessment should be conducted for the TPP. As the IRS enhances return processing filters and catches more fraudulent returns at the time of filing, criminals have become more sophisticated at faking taxpayers' identities so they can evade those filters and successfully obtain fraudulent refunds. A key

element in our efforts to improve protections for existing online tools and future ones is the development of a strong, coordinated, and evolving authentication framework. This framework will enable us to require multifactor authentication for all online tools and applications that warrant a high level of assurance. The IRS recently created a new position, the IRS Identity Assurance Executive, to lead in the development of our service-wide approach to authentication. We have also engaged with the U.S. Digital Service, which uses the best of product design, engineering practices, and technology professionals to build effective, efficient, and secure digital channels to transform the way government works for taxpayers.

Responses to your specific recommendations are enclosed. If you have any questions, please contact Ken Corbin, Director, Return Integrity and Compliance Services, Wage and Investment Division, at (404) 338-9042.

Sincerely,

John M. Dalrymple

Deputy Commissioner for Services and Enforcement

Enclosure

---

Page 4

Enclosure

Recommendations

#### RECOMMENDATION 1

To further deter noncompliance in the Taxpayer Protection Program, we recommend that the Commissioner of Internal Revenue take the following two actions, in accordance with OMB and NIST e-authentication guidance:

- Conduct an updated risk assessment to identify new or ongoing risks for TPP's online and phone authentication options, including documentation of timeframes for conducting the assessment, and
- Implement appropriate actions to mitigate risks identified in the assessment.

COMMENT

The IRS will conduct an updated e-authentication risk assessment for the Taxpayer Protection Program's (TPP) online e-authentication application. As it has in the past, the IRS will follow OMB M-04-04 and NIST 800-63 R2 guidelines when conducting the TPP e-authentication risk assessment to determine an assurance level commensurate with sensitivity of data or transaction type for web applications. To the extent that TPP- assigned contact representatives continue to use a web interface, that portion of telephonic contact will also be included in thee-authentication risk assessment.

#### RECOMMENDATION 2

To improve the quality of the Taxonomy's IDT refund fraud estimates, we recommend that the Commissioner of Internal Revenue take the following two actions:

- Remove refund thresholds from criteria used to develop IRS's refunds-paid estimates, and
- Utilize return-level data, where available, in order to reduce overcounting and improve the quality and accuracy of the refunds-prevented estimates.

#### COMMENT

The IRS reduced one of two thresholds (Lower Limit) for IDT 1, 2, and 3 in the Tax Year 2014 modeling dataset. This, in turn, will result in the reporting of additional returns outside current thresholds. The risk in the remaining threshold is mitigated because the IRS manually reviews returns outside of the remaining threshold (Upper Limit).

Return-level data and the IDT Global Report are not mutually exclusive. The Global

Report does use estimates from return-level data to provide values for the Confirmed Refund Protected Dashboard section of the Global Report (among other sections). The IDT Taxonomy uses the Global IDT Report because it is the report used by IRS leadership to see the impact of counter-IDT efforts (on a monthly basis). Since we

Data  
Tables/Accessible  
Text

**Accessible Text for Figure 1: Examples of How Identity Thieves Obtain Personally Identifiable Information**

1. Purchase personally identifiable information
2. Hack into government or commercial systems
3. Recruit insiders

**Data Table for Highlights Figure and Figure 4: IRS Estimates of Attempted Identity Theft Refund Fraud, 2014**

Total attempted identity theft (IDT) refund fraud estimated by IRS in 2014: \$25.6 billion

	Percentage	Dollars in billion
Percentage of IDT refunds prevented or recovered	88%	\$22.5
Percentage of IDT refunds paid	12%	\$3.1

---

# Related GAO Products

---

*2016 Annual Report: Additional Opportunities to Reduce Fragmentation, Overlap, and Duplication and Achieve Other Financial Benefits.* [GAO-16-375SP](#). Washington, D.C.: April 13, 2016.

*Information Security: IRS Needs to Further Improve Controls over Financial and Taxpayer Data.* [GAO-16-398](#). Washington, D.C.: March 28, 2016.

*Financial Audit: IRS's Fiscal Years 2015 and 2014 Financial Statements.* [GAO-16-146](#). Washington, D.C.: November 12, 2015.

*Information Security: IRS Needs to Continue Improving Controls over Financial and Taxpayer Data.* [GAO-15-337](#). Washington, D.C.: March 19, 2015.

*High-Risk Series: An Update.* [GAO-15-290](#). Washington, D.C.: February 11, 2015.

*Identity Theft and Tax Fraud: Enhanced Authentication Could Combat Refund Fraud, but IRS Lacks an Estimate of Costs, Benefits and Risks.* [GAO-15-119](#). Washington, D.C.: January 20, 2015.

*Identity Theft: Additional Actions Could Help IRS Combat the Large, Evolving Threat of Refund Fraud.* [GAO-14-633](#). Washington, D.C.: August 20, 2014.

*Financial Audit: IRS's Fiscal Years 2013 and 2012 Financial Statements.* [GAO-14-169](#). Washington, D.C.: December 12, 2013.

*Internal Revenue Service: 2013 Tax Filing Season Performance to Date and Budget Data.* [GAO-13-541R](#). Washington, D.C.: April 15, 2013.

*Identity Theft: Total Extent of Refund Fraud Using Stolen Identities is Unknown.* [GAO-13-132T](#). Washington, D.C.: November 29, 2012.

*Financial Audit: IRS's Fiscal Years 2012 and 2011 Financial Statements.* [GAO-13-120](#). Washington, D.C.: November 9, 2012.

*Taxes and Identity Theft: Status of IRS Initiatives to Help Victimized Taxpayers.* [GAO-11-721T](#). Washington, D.C.: June 2, 2011.

*Taxes and Identity Theft: Status of IRS Initiatives to Help Victimized Taxpayers.* [GAO-11-674T](#). Washington, D.C.: May 25, 2011.

---

Related GAO Products

---

*Tax Administration: IRS Has Implemented Initiatives to Prevent, Detect, and Resolve Identity Theft-Related Problems, but Needs to Assess Their Effectiveness.* [GAO-09-882](#). Washington, D.C.: September 8, 2009.

---

---

## GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

---

## Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (<http://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <http://www.gao.gov> and select "E-mail Updates."

---

## Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

---

## Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#).  
Subscribe to our [RSS Feeds](#) or [E-mail Updates](#).  
Listen to our [Podcasts](#) and read [The Watchblog](#).  
Visit GAO on the web at [www.gao.gov](http://www.gao.gov).

---

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <http://www.gao.gov/fraudnet/fraudnet.htm>

E-mail: [fraudnet@gao.gov](mailto:fraudnet@gao.gov)

Automated answering system: (800) 424-5454 or (202) 512-7470

---

## Congressional Relations

Katherine Siggerud, Managing Director, [siggerudk@gao.gov](mailto:siggerudk@gao.gov), (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

---

## Public Affairs

Chuck Young, Managing Director, [youngc1@gao.gov](mailto:youngc1@gao.gov), (202) 512-4800  
U.S. Government Accountability Office, 441 G Street NW, Room 7149  
Washington, DC 20548