



January 2015

IDENTITY THEFT AND TAX FRAUD

Enhanced
Authentication Could
Combat Refund
Fraud, but IRS Lacks
an Estimate of Costs,
Benefits and Risks

GAO Highlights

Highlights of [GAO-15-119](#), a report to congressional requesters

Why GAO Did This Study

IRS estimated it prevented \$24.2 billion in fraudulent identity theft (IDT) refunds in 2013, but paid \$5.8 billion later determined to be fraud. 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 an identity thief uses a legitimate taxpayer's identifying information to file a fraudulent tax return and claims a refund.

GAO was asked to review IRS's efforts to combat IDT refund fraud. This report, the second in a series, assesses (1) the quality of IRS's IDT refund fraud cost estimates, and (2) IRS's progress in developing processes to enhance taxpayer authentication.

GAO compared IRS's IDT estimate methodology to *GAO Cost Guide* best practices (fraud is a cost to taxpayers). To assess IRS's progress enhancing authentication, GAO reviewed IRS documentation and interviewed IRS officials, other government officials, and associations representing software companies, return preparers, and financial institutions.

What GAO Recommends

GAO recommends IRS improve its fraud estimates by (1) reporting the inherent imprecision and uncertainty of estimates, and (2) documenting the underlying analysis justifying cost-influencing assumptions. In addition, IRS should estimate and document the economic costs, benefits and risks of possible options for taxpayer authentication. IRS agreed with GAO's recommendations and provided technical comments that GAO incorporated, as appropriate.

View [GAO-15-119](#). For more information, contact James R. White, (202) 512-9110, whitej@gao.gov

January 2015

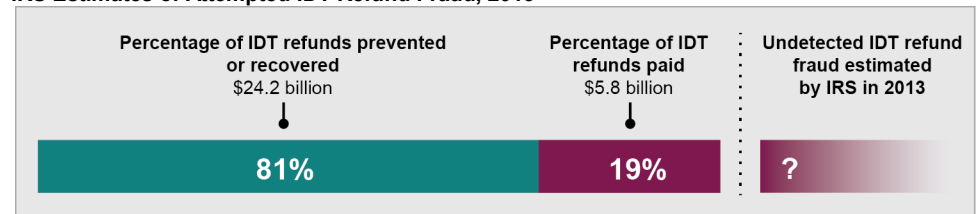
IDENTITY THEFT AND TAX FRAUD

Enhanced Authentication Could Combat Refund Fraud, but IRS Lacks an Estimate of Costs, Benefits and Risks

What GAO Found

Identity Theft (IDT) Refund Fraud Cost Estimates. The Internal Revenue Service's (IRS) fraud estimates met several *GAO Cost Guide* best practices, such as documenting data sources and detailing calculations. However, the estimates do not reflect the uncertainty inherent in measuring IDT refund fraud because they are presented as point estimates. Best practices suggest that agencies assess the effects of assumptions and potential errors on estimates. Officials said they did not assess the estimates' level of uncertainty because of resource constraints and methodological challenges. Because making different assumptions could affect IDT fraud estimates by billions of dollars, a point estimate (as opposed to, for example, a range) could lead to different decisions about allocating IDT resources. 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.

IRS Estimates of Attempted IDT Refund Fraud, 2013



Source: GAO analysis of IRS data. | GAO-15-119

While IRS's fraud estimates note the relevant cost assumptions used to develop estimates, they do not provide the rationale or analysis to support them. Officials stated they did not document the rationale because of the time and resources required. Best practices suggest that agencies should document assumptions. Given the evolving nature of IDT refund fraud, documenting assumptions' rationale would help IRS management and policymakers determine whether the assumptions remain valid or need to be updated.

Taxpayer Authentication. IRS recently created a group aimed at centralizing several prior ad hoc efforts to authenticate taxpayers across its systems. IRS's planning documentation contains goals and short- and long-term priorities (including implementation plans). However, a commitment to cost, benefit and risk analysis is not documented in the group's short- and long-term priorities. The draft planning documentation makes no mention of where such analyses would be included in IRS's priorities. Office of Management and Budget guidance states that agencies should use cost-benefit analyses that consider alternatives to promote efficient resource allocation and that agencies should ensure that authentication processes provide the appropriate level of assurance by assessing risks. Without analysis of costs, benefits and risks, IRS and Congress will not have quantitative information that could inform decisions about whether and how much to invest in the various authentication options. Cost, benefit and risk estimates for authentication would have the additional benefit of allowing comparisons with other options for combating IDT refund fraud. IDT options could have significant costs for taxpayers and IRS, so more information about the tradeoffs would help inform IRS and congressional decision making.

Contents

Letter		1
	Background	4
	<i>Taxonomy</i> Met Several Best Practices for Cost Estimating, but It Could Better Explain Assumptions and Reflect Inherent Uncertainty	12
	IRS Is Beginning to Implement One New Pre-Refund Tool and Is Exploring Enhanced Taxpayer Authentication, but Lacks Information on Costs, Benefits and Risks	19
	Conclusions	26
	Recommendations	26
	Agency Comments and Our Evaluation	27
Appendix I	Objectives, Scope, and Methodology	29
Appendix II	Summary of Tools to Combat Identity Theft Refund Fraud	34
Appendix III	How Assumptions Affect <i>Identity Theft Taxonomy (Taxonomy)</i> Results – Two Examples	37
Appendix IV	Comments from the Internal Revenue Service	42
Appendix V	GAO Contact and Staff Acknowledgments	46
Related GAO Products		47
Tables		
	Table 1: Summary of GAO’s Assessment of <i>Taxonomy</i> Estimates Using the <i>GAO Cost Guide</i> , Filing Season 2013	13
	Table 2: Changes in IRS <i>Identity Theft Taxonomy</i> Estimates of IDT Refunds Paid, Filing Season 2013	15
	Table 3: List of Third Parties Interviewed	32

Table 4: Overview of Current and Potential IRS Tools Used to Combat Identity Theft Refund Fraud, by Processing Stage	34
Table 5: Potential Estimates of E-file Rejects Using Different IRS IDT Defenses, Calendar Year 2013	40

Figures

Figure 1: Detecting IDT After Refunds are Issued: Two Examples	7
Figure 2: Illustration of IRS <i>Identity Theft Taxonomy</i>	9
Figure 3: Updated IRS <i>Taxonomy</i> Estimates of Attempted Identity Theft Refund Fraud, Filing Season 2013	11
Figure 4: How Assumptions Affect <i>Taxonomy</i> Estimates Based on Data from Information Return Matching	38
Figure 5: Estimating Refunds Prevented Using E-file Rejects and Average Refunds, Filing Season 2013	40

Abbreviations

AGI	adjusted gross income
AUR	Automated Underreporter
DDb	Dependent Database
EFDS	Electronic Fraud Detection System
e-file	electronically file
<i>GAO Cost Guide</i>	<i>GAO Cost Estimating and Assessment Guide</i>
<i>Global Report</i>	<i>Refund Fraud and Identity Theft Global Report</i>
IDT	identity theft
IP PIN	Identity Protection Personal Identification Number
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
NSTIC	National Strategy for Trusted Identities in Cyberspace
OMB	Office of Management and Budget
PIN	Personal Identification Number
RRP	Return Review Program
SSN	Social Security number
<i>Taxonomy</i>	<i>IRS Identity Theft Taxonomy</i>
Treasury	Department of the Treasury
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.



January 20, 2015

The Honorable Orrin Hatch
United States Senate

The Honorable Ron Wyden
United States Senate

The Honorable Susan M. Collins
United States Senate

The Honorable Bill Nelson
United States Senate

The Honorable Paul Ryan
House of Representatives

Tax refund fraud associated with identity theft (IDT) is a complex and rapidly changing threat facing the nation's tax system. IDT refund fraud occurs when a refund-seeking identity thief obtains an individual's identifying information and uses it to file a fraudulent tax return.¹ IDT refund fraud burdens honest taxpayers who have had fraudulent tax returns filed in their name because they must deal with delayed refunds as they authenticate their identities with the Internal Revenue Service (IRS). Additionally, IDT refund fraud is an attractive target for criminals with a potentially high payoff. While the estimates have inherent uncertainty, IRS estimated that it prevented \$24.2 billion in fraudulent IDT refunds in filing season 2013. However, IRS also estimated, where data were available, that it paid \$5.8 billion in fraudulent IDT refunds.² Because of the difficulties in knowing the amount of undetected fraud, the actual amount could differ from these point estimates.³

¹This 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.

²For more information, see GAO, *Identity Theft: Additional Actions Could Help IRS Combat the Large, Evolving Threat of Refund Fraud*, [GAO-14-633](#) (Washington, D.C.: Aug. 20, 2014).

³A point estimate is a population estimate that is presented as a single statistic.

This is the second in a series of our reports on IDT refund fraud. In August 2014, we issued a report describing what IRS knew about the extent of IDT refund fraud and identifying additional actions IRS could take to combat IDT refund fraud using third-party information.⁴ One action that the first report focused on was matching wage information that IRS receives from employers (on Form W-2, *Wage and Tax Statement (W-2)*) to tax returns before issuing refunds. While there is no “silver bullet” for combating IDT refund fraud, IRS officials told us that pre-refund W-2 matching could prevent billions of dollars in estimated IDT refund fraud; however, pre-refund matching would have costs. We noted that pre-refund W-2 matching would likely require some combination of accelerated due dates for information returns, delayed start of the annual tax filing season, delayed refund issuance, and investments in IRS information systems with the capability of doing real-time matching. We found that IRS had not considered how to implement such changes, including identifying their costs and benefits. We recommended that the agency estimate the costs and benefits to inform a discussion about whether to proceed. In November 2014, IRS reported that it had convened an internal working group to address our recommendations and that it anticipated implementing our recommendations by July 2015.

IRS has other pre-refund options for preventing IDT refund fraud. Two options that the agency is exploring are (1) tracking device identification numbers to determine when multiple returns are filed from the same device (e.g., the same laptop computer), and (2) authenticating the identity of a taxpayer before issuing a refund through the use of security questions, passwords, and other techniques.⁵

Within this context, you asked us to continue examining IRS’s efforts to combat IDT refund fraud. This report assesses (1) the quality of the IRS *Identity Theft Taxonomy’s (Taxonomy)* estimates of the cost of IDT refund fraud, and (2) IRS’s progress in developing processes to track device identification numbers and to enhance taxpayer authentication.⁶

⁴[GAO-14-633](#).

⁵Device identification is the unique number associated with an individual device, such as a laptop computer, used to electronically file a return.

⁶The *Taxonomy* estimates the number and cost of identified IDT refund fraud cases where (1) IRS prevented or recovered the fraudulent refunds, and (2) paid the fraudulent refunds.

To assess the quality of the *Taxonomy's* estimates of IDT-related refund fraud, we reviewed the *Taxonomy's* methodology for filing season 2013 and evaluated it against selected best practices in the *GAO Cost Estimating and Assessment Guide* that were applicable to the *Taxonomy* and consistent with IRS and Office of Management and Budget (OMB) information quality guidelines.⁷ Appendix I explains our scope and methodology and provides a summary of best practices selected. 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 discussed the criteria with IRS officials, who generally agreed with their applicability to the *Taxonomy*.⁸ We conducted manual data testing for obvious errors and compared underlying data to IRS's *Refund Fraud & Identity Theft Global Report*. We also interviewed IRS officials to better understand the methodology IRS used to create the estimates.

To assess IRS's progress in developing processes to track device identification numbers and to enhance taxpayer authentication, we reviewed *Internal Revenue Manual* sections detailing IRS's Identity Protection Program, and IRS documentation for several tools developed to combat IDT refund fraud. These included the Identity Protection Personal Identification Number (IP PIN), device identification, and other efforts related to identity authentication. We compared IRS's authentication group's planning documentation to OMB's guidance on cost-benefit analyses, as well as OMB and National Institute for Standards and Technology (NIST) guidance on assessing levels of assurance for electronic authentication.⁹ We also interviewed officials from NIST and associations representing software companies, return preparers, and financial institutions. To help ensure our analysis covered a variety of viewpoints, we selected a nonprobability sample of 18

⁷GAO, *GAO Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs*, [GAO-09-3SP](#) (Washington, D.C.: March 2009) and OMB, *Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies*, (Washington, D.C.: October 2001), accessed September 25, 2014, http://www.whitehouse.gov/omb/fedreg_final_information_quality_guidelines.

⁸For details, see appendix I.

⁹OMB, *E-Authentication Guidance for Federal Agencies*, M-04-04 (Washington, D.C.: Dec. 16, 2003); *Circular A-94: Guidelines and Discount Rates for Benefit Cost Analysis of Federal Programs* (Washington, D.C.: 1992); and NIST, *Electronic Authentication Guideline*, Special Publication 800-63-2, (August 2013).

associations and stakeholders with differing positions and characteristics based on IRS documentation and suggestions, our prior work, and other information. Because we used a nonprobability sample, the views of these associations are not generalizable to all potential third parties. We then communicated with IRS offices to determine the feasibility of various options and the challenges of pursuing them. See appendix I for details on our scope and methodology.

We conducted this performance audit from August 2013 to January 2015 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

Identity Theft Refund Fraud – Key Components

IDT refund fraud occurs in the context of several inter-related issues: the vulnerability of personal information, thieves' ability to exploit IRS's current compliance model, and the attractiveness of IDT refund fraud as a target.

Theft of Personal Information. To successfully commit IDT refund fraud, thieves must exploit various sources of information to steal or otherwise obtain individuals' identities. According to an official in IRS's Criminal Investigation division, the sources of stolen identities are limitless. The Department of Justice has prosecuted cases ranging from an employee stealing information from his employer to organized cyber attacks that infiltrate computer systems.

Exploitation of IRS Compliance Checks. After obtaining personal information belonging to legitimate taxpayers (or to individuals who do not have a tax filing obligation), identity thieves use this information to file fraudulent tax returns claiming refunds. Identity thieves are often able to exploit what IRS officials call a "look back" compliance model: rather than holding refunds until all compliance checks can be completed, IRS issues refunds after doing some selected, automated reviews of taxpayer-

submitted information (see text box). IRS is under pressure from taxpayers who expect to receive their refunds quickly.¹⁰ As a result, IRS normally issues refunds before matching tax returns to third-party information returns (such as W-2 data).

Examples of automated reviews used

- Matching name and Social Security number (SSN)
- Correcting obvious errors—such as mathematical mistakes or exceeding the statutory limits of deductions and credits.

Source: GAO analysis of IRS documents. | GAO-15-119

Attractiveness of IDT Refund Fraud. IDT refund fraud crimes often involve large criminal enterprises that exploit the speed and relative anonymity of preparing and filing tax returns. For this reason, they are difficult to prosecute, according to the Department of Justice.

IRS's Current IDT Refund Fraud Response

In light of the complexity and fluidity of this threat, IRS addressed refund fraud and IDT in its strategic plan, identifying both issues as major challenges facing the nation's tax system over the next several years (see text box).¹¹

IRS: Addressing the Threat of Refund Fraud and Identity Theft

"Assuring the accuracy of refunds and the security of taxpayer data remain our priorities going forward. We are committed to stopping this threat to tax administration, protecting our government's revenue and safeguarding the identity of all taxpayers. We must bolster our efforts to prevent refund fraud and identity theft before they happen."

Source: IRS *Strategic Plan: FY2014-2017*. | GAO-15-119

The plan further states that IRS is committed to building a stronger identity authentication process that will enable secure, timely processing of tax returns and improve other service interactions. IRS has also identified several strategic objectives relevant to its efforts to combat identity theft, including

¹⁰IRS's "Where's My Refund" website had about 201 million inquiries in fiscal year 2013, according to IRS data. For 2014, IRS announced that it would generally issue refunds in less than 21 days after receiving a tax return.

¹¹IRS, *Strategic Plan: FY2014-2017*, (Washington, D.C.: June 2014).

-
- balancing the speed of refund delivery with the need to verify taxpayers' identities; and
 - using third-party data, risk modeling, and a historical view of taxpayer interactions to prevent fraud before issuing refunds.

Further, IRS has allocated more than 3,000 employees to combat IDT refund fraud, including assigning staff to help IDT victims resolve their accounts. The agency has also requested an additional \$64.9 million in its fiscal year 2015 budget request for staffing and advanced technologies to support its continued IDT and refund fraud efforts.

In addition to identifying IDT refund fraud as a major issue and requesting additional resources, IRS has developed a number of tools to address IDT refund fraud throughout the tax return filing process—and has done so amidst budget reductions and other challenges.¹² IRS's response to IDT refund fraud includes efforts to authenticate taxpayer identities as well as several tools used to detect and prevent IDT refund fraud, as described below (see appendix II for more detail on these IDT refund fraud tools).

Authenticating Taxpayer Identities. IRS has enhanced its authentication efforts to combat IDT refund fraud. For example, IRS provides IP PINs to past IDT victims who have confirmed their identities with IRS. IP PINs help prevent future IDT refund fraud because, once issued, the IP PIN must accompany an electronically filed (e-file) tax return.¹³ In addition, IRS conducts authentication checks on returns flagged by IDT and fraud filters. If flagged, IRS stops processing the return and sends a letter asking the taxpayer to confirm his or her identity. IRS then confirms the taxpayer's identity by asking for personal information, such as the taxpayer's previous addresses, mortgage lender, and family members.

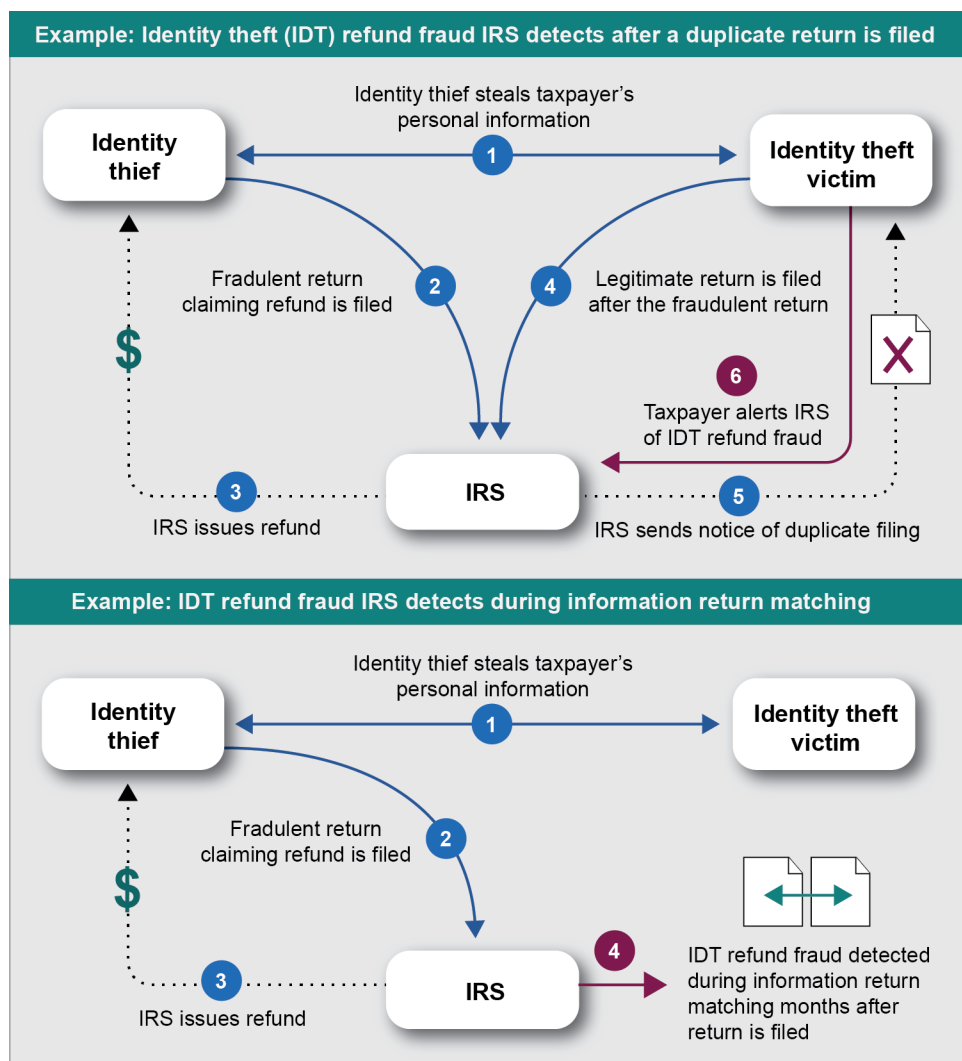
Taxpayer Alerts. Often, IRS becomes aware of IDT refund fraud when a legitimate taxpayer alerts IRS of an inability to e-file. Specifically, in cases where an identity thief has already e-filed a return using the taxpayer's

¹²Since 2010, the agency has absorbed approximately \$900 million in budget cuts while also facing an increasing workload due to legislative mandates, priority programs—such as the implementation and administration of various tax provisions enacted in the Patient Protection and Affordable Care Act—and IDT refund fraud.

¹³See [GAO-14-633](#) for more details on IRS's IP PIN program.

name and Taxpayer Identification Number—such as an SSN—IRS’s e-file system will reject the second, duplicate return (top of figure 1), thus preventing the legitimate taxpayer from filing. IRS officials are aware when their e-file system rejects returns; however, they do not know if the rejections are due to IDT refund fraud unless further investigation is conducted.

Figure 1: Detecting IDT After Refunds are Issued: Two Examples



Source: GAO analysis of IRS documents. | GAO-15-119

Note: In the examples, numbers represent the order in which these actions occur. Examples in the graphic do not include instances where IRS detects IDT refund fraud and prevents a refund.

Information Return Matching. IRS also finds IDT refund fraud as part of the Automated Underreporter (AUR) program, which matches tax return data to information returns, such as the W-2. These information returns are provided by third parties such as employers, financial institutions, and others. In many cases, IRS does not receive the information returns until well after the tax return and refund are processed (bottom of figure 1). In these types of cases, the legitimate taxpayer may not be aware of a stolen identity until after receiving a notice indicating that the income (or payment information) IRS has on file does not match the information reported on the tax return. We previously found that these post-refund compliance checks can take a year or more to complete, which can be a burden to taxpayers who receive a notice.¹⁴ IRS officials acknowledge that the longer the delay between filing a tax return and receiving an IRS notice, the harder it can be for taxpayers to locate tax records or other information necessary to respond to IRS.

Fraud Filters. IRS also uses IDT and other fraud filters to detect IDT refund fraud. These filters are computerized automatic checks that screen returns using characteristics that IRS has identified in previous IDT refund fraud schemes. The filters also search for clusters of returns with similar characteristics, such as the same bank account or address, which could indicate potential fraud. Two of the tax-administration systems employing filters are the Dependent Database (DDb) and Electronic Fraud Detection System (EFDS).¹⁵ IRS is also developing the Return Review Program (RRP) to replace EFDS. In April 2014, IRS began a pilot of one of RRP's planned fraud detection capabilities focused on detecting IDT refund fraud (e.g., RRP's IDT model).¹⁶ IRS officials said that they plan to use RRP's IDT model on all returns in filing season 2015. Returns flagged by the RRP IDT model will go through the same process as returns flagged by other filters (as previously described).

¹⁴GAO, *Tax Refunds: IRS is Exploring Verification Improvements, but Needs to Better Manage Risks*, [GAO-13-515](#) (Washington, D.C.: June 4, 2013).

¹⁵DDb incorporates IRS, Department of Health & Human Services, and Social Security Administration data to identify compliance issues involving IDT, refundable credits, and prisoners. EFDS is a system built in the mid-1990s to detect taxpayer fraud.

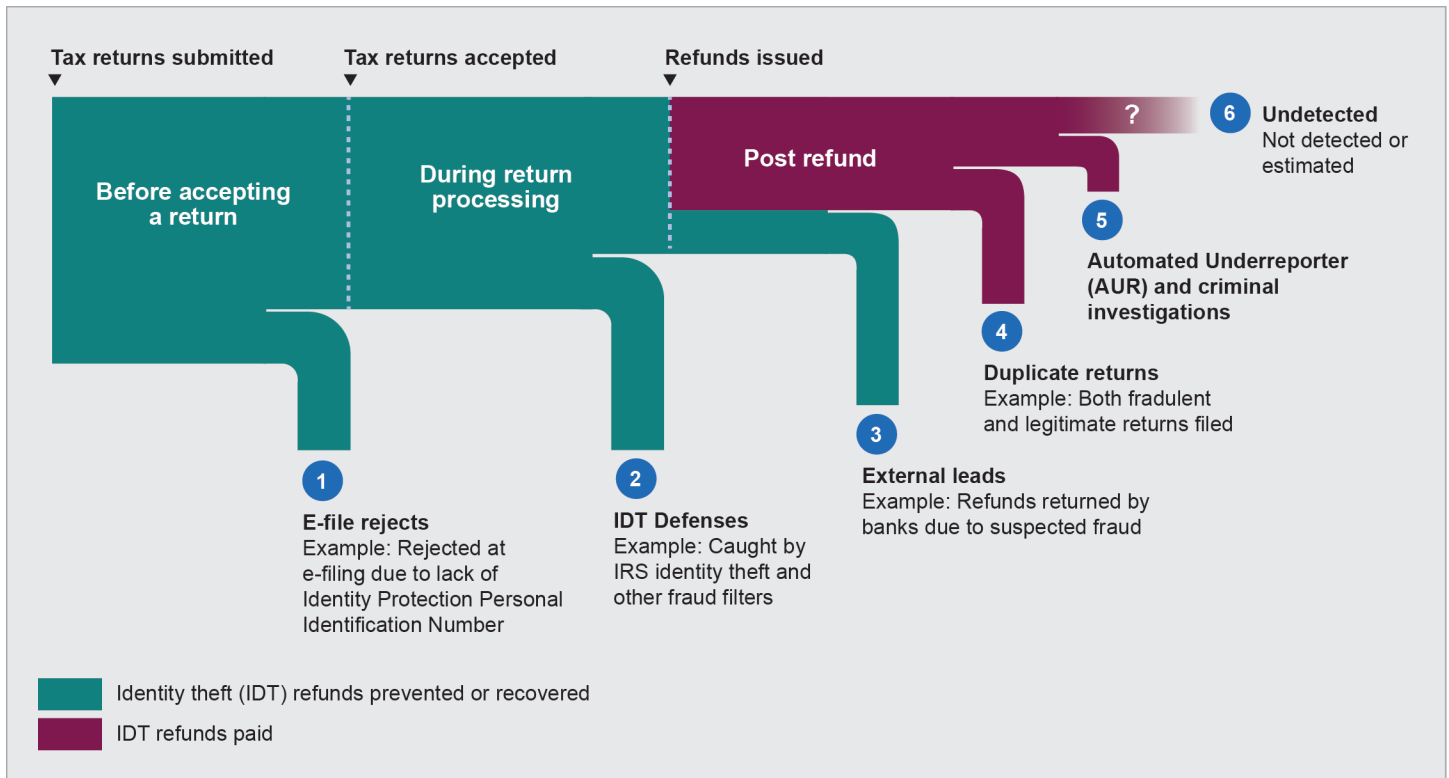
¹⁶IRS has paused further RRP development due to budget constraints and a need to ensure alignment of RRP goals with IRS's strategic vision for IDT and refund fraud detection, among other reasons, according to IRS officials.

IRS's Efforts to Identify and Monitor the Extent of IDT Refund Fraud

According to IRS officials, a vital component in the agency's strategy to identify IDT refund fraud is its *Identity Theft Taxonomy (Taxonomy)*. This research-based effort has several objectives, including (1) providing information to internal and external stakeholders about the effectiveness of IRS's IDT defenses, (2) helping IRS identify IDT trends and evolving risks, and (3) refining IDT filters to better detect potentially fraudulent returns while reducing the likelihood of flagging legitimate tax returns.

Taxonomy Methodology. Consisting of a matrix of IDT refund fraud categories (see figure 2), 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 six categories associated with IDT detection strategies. These strategies 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 2: Illustration of IRS *Identity Theft Taxonomy*



Source: GAO analysis of IRS *Taxonomy*. | GAO-15-119

Taxonomy Categories. Estimates in categories 1-3 are based on IRS's *Refund Fraud & Identity Theft Global Report (Global Report)*, which consolidates IRS administrative records of known IDT refund fraud.¹⁷ Category 4 estimates are based on duplicate returns, where IRS has received both a fraudulent IDT return and a legitimate return. Category 5 estimates are based on cases identified as part of a criminal investigation or as part of the AUR program. To estimate the AUR portion of category 5, IRS developed assumptions based on its analysis of the characteristics of past IDT refund fraud; IRS then used these assumptions to identify which information return mismatches were likely IDT returns.¹⁸ Category 6 represents undetected IDT returns.

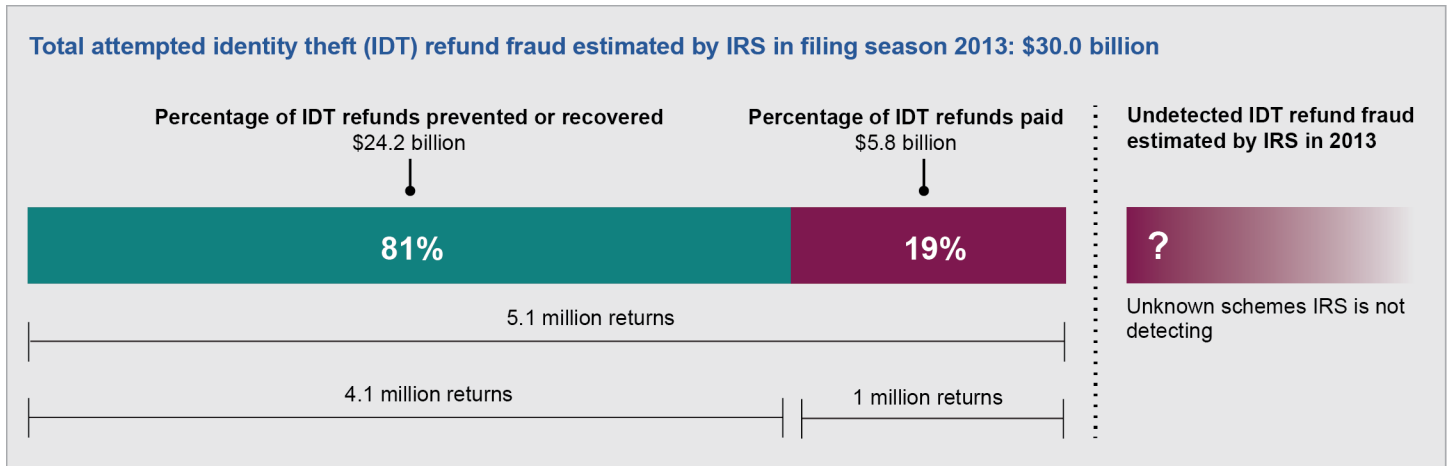
Current Taxonomy Estimates. Based upon its *Taxonomy*, IRS estimated that \$30 billion in IDT refund fraud was attempted in filing season 2013 (see figure 3). Of this attempted amount of IDT refund fraud, IRS estimated that it prevented or recovered \$24.2 billion (81 percent) of the estimated total. IRS also estimated it paid \$5.8 billion (19 percent) in IDT refunds on 1 million IDT returns during the same time frame.¹⁹ *Taxonomy* estimates do not include the amount of IDT refund fraud from schemes IRS cannot detect (e.g., schemes that involve reported income that IRS cannot confirm during information return matching).

¹⁷The *Global Report* tracks information about identity theft incidents and IRS detection and resolution efforts using multiple sources within IRS.

¹⁸IRS officials must develop these assumptions because without conducting a tax return audit, it is impossible for officials to determine whether mismatches are IDT returns or other noncompliant returns (i.e., a legitimate taxpayer makes a mistake or purposely files a noncompliant return).

¹⁹This figure is an update to a similar figure that appeared in [GAO-14-633](#). Since we issued [GAO-14-633](#), IRS's estimate of IDT refunds paid increased from \$5.2 billion to \$5.8 billion, as will be discussed later.

Figure 3: Updated IRS *Taxonomy* Estimates of Attempted Identity Theft Refund Fraud, Filing Season 2013



Source: GAO analysis of IRS data. | GAO-15-119

Administration Prioritizes Identity Theft and Authentication Efforts

In October 2014, the administration announced a plan to combat identity theft and further strengthen the security of personal identifying information maintained by the government.²⁰ The plan is intended to ensure that all agencies making personal data accessible to citizens online will require the use of multiple authentication steps and will have an effective identity proofing process. National Security Council staff, the Office of Science and Technology Policy, and the Office of Management and Budget (OMB) are tasked with developing this plan by January 2015, and relevant agencies shall complete any required implementation steps set forth in this plan by April 2016. Therefore, while this plan may aid IRS in its efforts to prevent identity theft, any implementation of the plan at the agency level is still a few years away.

²⁰Administration of Barack Obama, *Executive Order 13681, Improving the Security of Consumer Financial Transactions* (Washington, D.C.: Oct. 17, 2014).

Taxonomy Met Several Best Practices for Cost Estimating, but It Could Better Explain Assumptions and Reflect Inherent Uncertainty

Taxonomy Documented Data and Methodology

By providing insight into how IDT refund fraud is evading IRS defenses, estimates inform IRS decision making about how to improve fraud filters and other detection efforts. Objective estimates may also inform congressional decision making about IRS resources. To ensure that IRS information reporting is objective, the agency developed information quality guidelines.²¹ Objectivity involves ensuring that information is reliable, accurate, and unbiased, as defined in OMB information quality guidelines.²² Further, OMB quality guidelines state that, where appropriate, supporting data should include full, accurate, transparent documentation, and should disclose error sources affecting data quality.

We evaluated *Taxonomy* estimates against selected *GAO Cost Estimating and Assessment Guide* (*GAO Cost Guide*) best practices that (1) are related to OMB's definition of objectivity, and (2) are applicable to the *Taxonomy*.²³ These best practices are intended to ensure the reliability of estimates—a key component of OMB's definition of objectivity. While IRS is not required to follow the *GAO Cost Guide* best practices, following such practices could help the agency meet OMB and IRS information quality guidelines and could improve the reliability of IDT

²¹IRS developed these guidelines pursuant to the Treasury and General Government Appropriations Act for Fiscal Year 2001 (P.L. 106-554, § 515).

²²OMB, *Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies*, (Washington, D.C.: October 2001), accessed September 25, 2014, http://www.whitehouse.gov/omb/fedreg_final_information_quality_guidelines.

²³GAO-09-3SP.

refund fraud estimates. We assessed the extent to which IRS provided evidence that the *Taxonomy* met each best practice and assigned ratings based on a five-point scale (Met, Substantially met, Partially met, Minimally met, or Not met). See appendix I for details on how we conducted our assessment.

As shown in table 1, the *Taxonomy* met several *GAO Cost Guide* best practices. IRS documented the *Taxonomy*'s source data, identified the methodology used to develop the estimate, and described how the estimate was developed. With regard to the calculation of *Taxonomy* estimates, our data reliability testing did not find calculation errors or other mistakes.²⁴

Table 1: Summary of GAO's Assessment of *Taxonomy* Estimates Using the *GAO Cost Guide*, Filing Season 2013

Best practice characteristics	Assessment of whether best practices are met
Captures the source data used.	The <i>Taxonomy</i> documentation captures the source data used. (Met)
Describes in sufficient detail the calculations performed and the estimating methodology used to derive each element's cost.	The <i>Taxonomy</i> documentation describes in detail the calculations performed and the methodology used to derive each <i>Taxonomy</i> category. (Met)
Describes step by step how the estimate was developed so that a cost analyst unfamiliar with the program could understand what was done and replicate it.	The <i>Taxonomy</i> documentation describes step by step how the estimate was developed. (Met)
Contains few mistakes.	Our data reliability testing did not find calculation errors or other mistakes. ^a (Met)
Is regularly updated to reflect significant changes in the methodology.	IRS officials regularly update the <i>Taxonomy</i> methodology to better reflect evolving IDT refund fraud schemes and to improve the accuracy of <i>Taxonomy</i> estimates. (Met)
Includes all relevant costs.	The filing season 2013 <i>Taxonomy</i> estimates the number of cases of IDT refund fraud and associated costs throughout the life cycle of a tax return. Methodology improvements made filing season 2013 estimates more comprehensive by including categories of IDT returns that had not been included in filing season 2012 estimates. However, IRS has been unable to estimate the amount of IDT refund fraud from undetected schemes, such as when there is no information reporting to verify income. While IRS has considered a different approach to estimating the costs of undetected IDT, administrative costs and taxpayer burden are likely to make these approaches impractical. (Partially met)

²⁴There may be some types of error that our data reliability testing was unable to detect. For example, we cross-checked *Taxonomy* estimates against the *Global Report*; however, if the *Global Report* itself contains errors, our data reliability testing would not detect these errors.

Best practice characteristics	Assessment of whether best practices are met
Provides evidence that the cost estimate was reviewed and accepted by management.	The <i>Taxonomy</i> documentation does not provide evidence that the cost estimate was reviewed and accepted by management. However, IRS officials stated they are working on a new process to document management review and approval. (Partially met)
Documents all cost-influencing ground rules and assumptions.	The <i>Taxonomy</i> documentation notes the assumptions used to develop the estimates. However, it does not provide the rationale or analysis supporting those assumptions. The assumptions likely result in overestimates for some categories and underestimates for others; however, methodology and data limitations make it unlikely that IRS will be able to account for this in the short term, if ever. (Partially met)
Includes a sensitivity analysis. ^b	While IRS conducted a sensitivity analysis for one part of the <i>Taxonomy</i> , it did not conduct sensitivity analyses for other categories. (Minimally met)
Includes a risk and uncertainty analysis. ^c	The <i>Taxonomy</i> acknowledges that there is uncertainty in the estimates. For example, IRS documentation states that <i>Taxonomy</i> estimates for one category do not include fraud that IRS currently cannot detect (e.g., schemes that involve reported income that IRS cannot confirm during information return matching). However, because of methodology and resource constraints, IRS did not conduct a risk and uncertainty analysis that would have illustrated the cumulative effect that assumptions have on the cost estimate, according to IRS officials. (Minimally met)
Results are not overly conservative or optimistic, and are based on an assessment of most likely costs.	The <i>Taxonomy</i> documentation explicitly documents a key uncertainty in its estimates: IDT refund fraud that IRS currently does not detect. However, because IRS did not conduct risk and uncertainty analyses for the numerical estimates it did produce, the level of uncertainty associated with the estimates is unclear. Presenting the <i>Taxonomy</i> as a point estimate does not reflect the inherent uncertainty of the estimate. (Minimally met)

Source: GAO analysis of IRS *Identity Theft Taxonomy* documentation, interviews with IRS officials, and GAO-09-3SP. | GAO-15-119

Note: We determined the overall assessment rating by assigning the following ratings: Did not meet—IRS provided no evidence that satisfies any of the best practice; Minimally met—IRS provided evidence that satisfies a small portion of the best practice; Partially met—IRS provided evidence that satisfies about half of the best practice; Substantially met—IRS provided evidence that satisfies a large portion of the best practice; and Met—IRS provided complete evidence that satisfies the entire best practice. See appendix I for a description of how we conducted our assessment.

^aThere may be some types of error that our data reliability testing was unable to detect. For example, we cross-checked *Taxonomy* estimates against the *Global Report*; however, if the *Global Report* itself contains errors, our data reliability testing would not detect these errors.

^bA 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.

^cRisk 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.

Methodology Changes Increased Fraud Estimates by \$1 Billion, and Officials are Developing a Process to Document Management Review

After initial development of the *Taxonomy* in 2013, IRS made methodology improvements that resulted in more comprehensive *Taxonomy* estimates. For example, the agency included categories of duplicate IDT returns that had not been in filing season 2012 estimates. IRS made these methodology changes to enable comparison across filing seasons in future years, and to respond to our data reliability questions, according to officials. As a result, 2013 filing season estimates of “IDT refunds paid” increased by about \$1 billion from an original estimate of \$4.8 billion to a revised estimate of \$5.8 billion (see table 2 for details).

Cost Guide Best Practice:

- Is regularly updated to reflect significant changes in the methodology.
- Includes all relevant costs.
- Provides evidence that the cost estimate was reviewed and accepted by management.

Source: GAO-09-3SP. | GAO-15-119

Table 2: Changes in IRS Identity Theft Taxonomy Estimates of IDT Refunds Paid, Filing Season 2013

Date	Estimate of IDT refunds paid	Amount increased from prior estimate	Reason for change
May 23, 2014 (original estimate)	\$4.8 billion	Not applicable	Not applicable
June 23, 2014	\$5.2 billion	\$0.4 billion	In response to our questions, IRS officials agreed that the <i>Taxonomy</i> 's methodology for counting returns should have included two categories of duplicate returns. Including these categories resulted in an increase in the amount of IDT refunds paid. We reported this figure in GAO-14-633 .
July 22, 2014	\$5.8 billion	\$0.6 billion	IRS officials said they updated the <i>Taxonomy</i> 's methodology to account for corrections within AUR data and to create a standard way of reporting estimates from year to year.

Source: GAO analysis of IRS Identity Theft Taxonomy and interviews with IRS officials. | GAO-15-119

IRS officials have considered using surveys to develop a more comprehensive estimate of unidentified IDT refund fraud, but have not been able to develop a survey method that would avoid significant taxpayer burden and administrative costs. Accordingly, while IRS has made several methodology changes and refinements to improve *Taxonomy* estimates, it is unlikely that IRS will be able to develop a completely comprehensive estimate, given potential administrative costs and other constraints.

While *Taxonomy* documentation does not provide evidence of managerial review, IRS officials stated that the former IRS Acting Commissioner reviewed and approved the *Taxonomy*. Officials told us they are working on a new process to document management review and approval.

Taxonomy Notes Relevant Cost Assumptions Used, but Does Not Provide the Rationale or Analysis Supporting the Assumptions

Cost Guide Best Practice:

- Documents all cost-influencing ground rules and assumptions.

Source: GAO-09-3SP. | GAO-15-119

Developing loss estimates of illicit activities is challenging because such activities are difficult to observe. For this reason, IRS makes various assumptions, including whether an information return mismatch is an IDT return.

Taxonomy documentation thoroughly details IRS’s assumptions. For example, the *Taxonomy* describes the assumptions used to develop its “refund paid” estimates in category 5, which are based on AUR data (see figure 2).²⁵ This part of the *Taxonomy* accounts for \$3.0 billion of the estimated \$5.8 billion in IDT refunds paid by IRS. However, the *Taxonomy* documentation for the AUR category does not provide information on the analysis or rationale used to develop the assumptions of past IDT refund fraud characteristics (see appendix III for examples showing how IRS assumptions affect *Taxonomy* results).

Given the evolving nature of IDT refund fraud, documenting *Taxonomy* assumptions and the rationale used to develop the assumptions would help IRS management and policymakers to determine whether the assumptions remain valid or need to be revised or updated. IRS officials acknowledged they could have better documented their analysis and rationale for choosing assumptions. They stated that IRS did not document its rationale for selecting assumptions because of the time and resources required.

Taxonomy assumptions also result in overestimates in some categories and underestimates in others. For example, while IRS’s estimate for refunds prevented includes e-file rejects that occurred due to an incorrect or missing Identity Protection Personal Identification Number (IP PIN) (see figure 2), legitimate taxpayers may also have their return rejected if they include an incorrect IP PIN, or forget to include an IP PIN on their tax return. In addition, the same return—regardless of whether the return is

²⁵The AUR program matches information returns to tax returns and pursues discrepancies.

filed by a legitimate taxpayer or an identity thief—can be rejected multiple times, which would result in an over-count of IDT refunds prevented. Officials said they do not collect data that would allow them to break out the amount of e-file rejects due to IDT refund fraud. According to IRS officials, the costs of collecting these data may outweigh the benefits, as it would require major changes to IRS information technology systems.

Point Estimates Do Not Reflect the *Taxonomy's* Inherent Uncertainty

Cost Guide Best Practice:

- Includes a sensitivity analysis.
- Includes a risk and uncertainty analysis.
- Results are not overly conservative or optimistic, and are based on an assessment of most likely costs.

Source: GAO-09-3SP. | GAO-15-119

To gain a better understanding of the effects that changing assumptions had on its estimates, IRS conducted a sensitivity analysis for category 5 “IDT refunds paid” estimates (which are based on AUR data from filing season 2013).²⁶ That analysis shows that making different assumptions could affect the estimate of category 5 IDT refunds paid by billions of dollars in either direction (see appendix III, example 1). However, IRS does not report a range or some other indication of the results of the sensitivity analysis when reporting the \$5.8 billion estimate for IDT refund fraud detected after refunds were issued. IRS officials stated that their goal in developing the *Taxonomy* was to achieve a level of precision that would allow them to assess the effectiveness of IRS IDT defenses.

Nor did IRS conduct sensitivity analyses for the other *Taxonomy* categories that include assumptions. Our analysis, shown in example 2 in appendix III, demonstrates that changes in these assumptions could affect estimates by billions of dollars. Also, IRS did not conduct a risk and uncertainty analysis showing the cumulative effect that assumptions have on the fraud estimate.²⁷ 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.

IRS officials stated that they did not conduct such analyses because of resource constraints and methodological challenges. Specifically, IRS officials stated that it would be methodologically difficult—if not impossible—to calculate uncertainty surrounding category 5 estimates

²⁶A 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.

²⁷Risk 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.

that are based on AUR data. However, officials acknowledged that these analyses are possible for other categories in the *Taxonomy*, such as categories that use average refund value assumptions, or assumptions about the percent of returns detected by IRS defenses that are IDT.²⁸

We recognize that conducting an uncertainty analysis will be challenging and add some costs; however, better reporting of what is already known from sensitivity analyses would not be costly. Reporting the uncertainty that is known already, and conducting further sensitivity analyses when not cost prohibitive, might help IRS communicate the complexities inherent in combating the evolving threat of IDT refund fraud. Reporting uncertainty, quantitatively if possible and otherwise qualitatively, could also give decision makers in Congress and IRS a more accurate understanding of what is known and not known about the extent of the IDT refund fraud problem. A point estimate, compared to a range or some other indication of uncertainty, could provide a false sense of precision leading to different decisions about how to allocate resources to combat IDT refund fraud.

Given methodological and resource constraints, there are various ways IRS could report the uncertainty in the IDT refund fraud estimates. One way would be to present a point estimate surrounded by quantitative estimates of the possible range. Another way would be to qualitatively describe the relative size of the uncertainty and the reasons for this uncertainty. For example, IRS could describe how changes in assumptions affect the *Taxonomy's* minimum, point, and maximum estimates.

²⁸For some IDT metrics used to develop *Taxonomy* estimates in categories 1-3, the *Global Report* provides detail on the volume of IDT returns but has no detail on the refunds associated with those returns. For example, the *Global Report* provides data on the number of e-filed returns rejected due to a missing or incorrect IP PIN, but does not have data on the refunds associated with those returns. In other cases, IRS defenses do not distinguish IDT from other types of fraud. For example, the Electronic Fraud Detection System (EFDS) detects fraudulent returns, but in some cases does not differentiate between whether the returns are IDT or noncompliant. Therefore, to develop its *Taxonomy* category 2 estimates, IRS develops assumptions on the percent of returns detected by EFDS that are IDT refund fraud.

IRS Is Beginning to Implement One New Pre-Refund Tool and Is Exploring Enhanced Taxpayer Authentication, but Lacks Information on Costs, Benefits and Risks

While it is likely that no one tool will stop all attempts at fraud, we have found that implementing strong preventive controls can help defend against invalid refunds, increasing public confidence and avoiding the difficult “pay and chase” aspects of recovering invalid refunds.²⁹ Recapturing a fraudulent refund after it is issued can be challenging—if not impossible—because identity thieves often spend or transfer the funds immediately, making them very difficult to trace. For this reason, IRS is in various stages of exploring several possible pre-refund tools. Three tools with significant potential are (1) pre-refund Form W-2, *Wage and Tax Statement* (W-2) matching (which we already noted was the subject of our August 2014 report), (2) device identification, and (3) improved taxpayer authentication.

IRS is Working with Tax Software Companies to Implement Device Identification

Based on suggestions from the tax software industry and internal stakeholders, IRS is beginning to implement device identification that would capture the unique number associated with the individual device, such as a laptop computer, used to e-file a return. IRS could use this information to determine when multiple fraudulent returns are filed from the same device.

In November 2014, IRS published guidance for e-file providers that outlined IRS’s plans to collect device identification numbers along with tax returns for filing season 2015.³⁰ IRS officials told us they will collect device identification numbers voluntarily for this first year. Beginning in filing season 2016, IRS plans to require these companies to submit a device identification number with each e-filed tax return.³¹

²⁹GAO, *Improper Payments: Remaining Challenges and Strategies for Governmentwide Reduction Efforts*, [GAO-12-573T](#) (Washington, D.C.: Mar. 28, 2012).

³⁰IRS, *Publication 1345, Handbook for Authorized IRS e-File Provider of Individual Income Tax Returns* (Washington, D.C.: Nov. 17, 2014). Authorized e-file providers are tax professionals who are accepted into the electronic filing program and who transmit tax return information to the IRS.

³¹IRS already requires all tax software companies to identify the particular software package used to prepare tax returns using a three-letter source code on all electronically prepared paper returns. This was a change IRS implemented as a result of our prior recommendation. See GAO, *Many Taxpayers Rely on Tax Software and IRS Needs to Assess Associated Risks*, [GAO-09-297](#) (Washington, D.C.: Feb. 25, 2009).

From a cost-benefit perspective, IRS's implementation of device identification appears justified. One important benefit of device identification is that it will enhance IRS's ability to monitor when multiple returns are filed from the same device or from devices previously associated with fraud. In addition, device identification analysis could aid in criminal investigations, according to officials from one software industry group we interviewed.

Device identification will impose minimal, if any, costs on taxpayers, third parties, or IRS. It will not require additional taxpayer action, according to IRS. In addition, IRS and tax software companies told us that while tax software companies already capture device identification numbers when a taxpayer is preparing a return, that information is not currently transmitted to IRS. In contrast to some other options IRS is considering, such as earlier W-2 matching, IRS can use current information technology systems and processes to implement the device identification tool. For example, the device identification number will be transmitted to IRS via existing return transmission processes for e-filed returns. IRS could also use its existing filters as a low-cost method of determining patterns of device usage.

IRS is Pursuing Improved Taxpayer Authentication to Prevent IDT Refund Fraud; However, the Agency Does Not Have a Plan to Assess Costs, Benefits and Risks

IRS's Current Authentication Tools Have Limitations

IRS has developed various personal identification numbers (PIN) to authenticate taxpayers' identities and help verify the legitimacy of tax returns (see text box). Typically, these PINs are used by taxpayers to sign e-filed tax returns. IRS programs its systems to not accept a tax return if a required PIN is missing or does not match agency records. However, according to our analysis of IRS information and interviews with experts from tax software companies and associations, IRS's current authentication tools (such as the e-file PIN) have limitations.

PINs and the Identity Authentication They Require

- *Self-select PIN* – Most taxpayers are eligible to use the Self-Select PIN. The Self-Select PIN requires taxpayers to provide their prior year’s adjusted gross income (AGI) amount or prior year’s self created PIN to authenticate the taxpayer’s identity.
- *E-file PIN* – If taxpayers do not have a self-select PIN or their prior year’s AGI, they can obtain an e-file PIN. The e-file PIN requires taxpayers to authenticate their name, SSN, date of birth, address, and filing status.
- *IP PIN* – IRS provides IP PINs to past IDT victims who have confirmed their identities with IRS, or to taxpayers who participated in a pilot program. In filing season 2014, IRS offered this pilot to taxpayers in Florida, Georgia, and the District of Columbia.

Source: GAO analysis of IRS documents. | GAO-15-119

- **Identity thieves may be able to falsely obtain e-file PINs.** Identity thieves can easily find the information needed to obtain an e-file PIN, allowing them to bypass some, if not all of IRS’s current automatic checks, according to our analysis and interviews with tax software and return preparer associations and companies.³² According to IRS, identity thieves can find identifying information through public records or other easily accessible sources.
- **Only a small number of taxpayers undergo knowledge-based authentication or receive IP PINs.** Knowledge-based authentication—a more intensive authentication process—uses questions about personal information that only the taxpayer should know to confirm taxpayers’ identities.³³ Examples of authentication questions are “Who is your mortgage lender?” or “Which of the following is your previous address?” IRS uses authentication questions to confirm the identities of taxpayers whose returns are flagged by IRS’s IDT and other fraud filters.³⁴ Only a limited number of returns—about 1 percent—are currently subject to this more intensive authentication process. IRS also uses authentication questions to confirm the identities of taxpayers who request an IP PIN. Because IRS did not advertise the IP PIN pilot, the participation rate for the pilot was low. According to IRS officials, as of July 31, 2014, IRS had

³²We asked an open-ended question about how IRS could combat IDT. Three of the six companies and associations offered this specific information. The others were silent on the e-file PIN.

³³Authentication questions can draw on information in public records databases (e.g., credit records) or from the individual’s tax records.

³⁴For returns flagged by fraud filters, IRS sends a letter asking the taxpayer to confirm his or her identity by calling IRS, by providing a written response, or by answering online authentication questions.

IRS Has Options for Improving Its Authentication Tools

received about 21,000 requests out of about 13.9 million eligible taxpayers (or about 0.15 percent of eligible taxpayers), in 2014. IDT thieves can also obtain and use credit bureau information to answer the authentication questions, according to IRS officials.

IRS officials and several third parties, including software providers and paid preparers, suggested IRS could enhance its taxpayer authentication approach by expanding some current tools and by exploring additional options. According to our review of IRS and third-party information, each of these options has strengths and weaknesses. Unlike the device identification tool, these options could require substantial changes to tax administration and may burden taxpayers by requiring individuals to track additional information or to take additional steps when filing a tax return. Similar to pre-refund W-2 matching, improved authentication tools could provide substantial benefits but require major investments in IRS systems and changes to work processes. One advantage of authentication is that it could be applicable to more tax returns than pre-refund W-2 matching, since W-2 matching only works for tax returns reporting wage income. Authentication options include:

- **Expanding the use of current authentication questions to a wider set of taxpayers.** IRS could use authentication questions for the entire individual taxpayer population or in conjunction with other tools. IRS is continually analyzing the effectiveness of its authentication questions, which may be a benefit if the program was expanded. However, IRS analysis of single filers whose returns were flagged by fraud filters and who answered authentication questions has shown limitations: some likely identity thieves were able to correctly answer authentication questions while some legitimate taxpayers were not.³⁵
- **Expanding the availability of the IP PIN pilot to additional taxpayers.** Currently, IP PIN distribution is limited to individuals who are IDT refund fraud victims or who participated in the IP PIN pilot. However, IRS is considering an expansion of the IP PIN to include more taxpayers. In responding to an open-ended question, 3 of the 18 associations we interviewed also suggested expanding the IP PIN

³⁵IRS found that 5 percent of the “high risk” group (likely identity thieves) correctly answered the authentication questions. In contrast, 19 percent of the “low risk” group (likely legitimate taxpayers) that attempted to authenticate did not correctly answer the questions. To develop this analysis, IRS categorized returns into “high risk” and “low risk” groups using characteristics such as whether tax return data matched information return data submitted by third parties.

pilot to all taxpayers as an optional effort.³⁶ An IP PIN provides an additional layer of security for taxpayers, according to IRS. However, the effectiveness of the IP PIN relies on the strength of authentication questions, which have the limitations described above. In addition, because taxpayers only use the IP PIN once a year when filing their returns, retrieving lost IP PINs creates additional burden for taxpayers and IRS.

- **Developing and issuing IRS or third-party credentials (e.g., username and password or tokens that generate random numbers) to taxpayers.** Under a credential system, taxpayers could actively confirm their identities through authentication questions and then receive a credential from IRS or a third party.³⁷ This credential could be required when filing taxes, and could also be used for other transactions. A study prepared for the National Institute for Standards and Technology (NIST) describes options for a credential system: an IRS-issued credential for filing taxes or a third-party-issued credential that could be used for other purposes (e.g., accessing an online bank account).³⁸ NIST found that improved authentication through a credential may help IRS more effectively combat IDT refund fraud, as it may allow IRS to target resources toward returns filed without a credential. However, obtaining a credential would involve some taxpayer burden. In addition, like the IP PIN, taxpayers could easily lose an IRS-issued credential because it would be used only when filing a tax return.
- **Implementing a risk-based authentication strategy that would select returns for additional authentication checks if the returns are high risk.** For example, IRS could match return information (e.g., name, address, SSN) against third-party databases to assess the risk that the identity has been stolen before IRS accepts the return for processing. High-risk returns would require the filer to answer authentication questions to confirm their identity, whereas low-risk

³⁶We asked an open-ended question about how IRS could combat IDT. Three of the companies and associations offered this specific information and one company recommended an alternative option. The others were silent on expanding the IP PIN.

³⁷A third-party issued credential would be aligned with standards established by the National Strategy for Trusted Identities in Cyberspace (NSTIC), a White House initiative to develop an online environment where organizations follow agreed upon standards to obtain and authenticate their digital identities.

³⁸NIST, *Planning Report 13-2, Economic Case Study: The Impact of NSTIC on the Internal Revenue Service* (July 2013).

IRS Is Creating an Authentication Group to Examine Options, but Lacks a Plan For Identifying and Assessing Tools

returns would be processed. According to one analytics company we interviewed, because this option could be an automated, computerized match that would not require any action from taxpayers, it would limit burden on low-risk taxpayers because they would not be subject to additional authentication checks. Although the analytics company official stated that this authentication option has been used by some states, he also acknowledged that there are no data available about its effectiveness in combating IDT refund fraud at the state level.

According to IRS officials, the agency is in the initial stages of creating an authentication group aimed at centralizing several prior ad hoc efforts to authenticate taxpayers across IRS services (e.g., online, telephone calls, walk-in services). While the group was not specifically designed in response to IDT refund fraud, improving authentication across IRS would likely advance IRS's ability to combat such fraud. IRS officials anticipate the group will consider options for improving authentication and will make recommendations to senior IRS executives. As of October 2014, the group was operating as a task team, with staff detailed from other IRS units. In its draft planning documentation, the authentication group outlined several initial high-level goals. Generally, they include:

- Centralize protection of IRS and taxpayers through integrated identity management;
- Centralize decisions and a strategic approach for authentication;
- Provide an avenue for tax administration through identity management;
- Provide an operational foundation for authentication;
- Provide a consistent operational approach to implementing authentication processes, including updating relevant *Internal Revenue Manual* sections;
- Improve the security of IRS interactions and transactions with internal and external stakeholders; and
- Coordinate the testing of authentication techniques (e.g., in-person or remote authentication through the Post Office or other venues).

The group has also documented short- and long-term priorities, including implementation plans. In recent discussions, agency officials said they would coordinate analysis of costs, benefits and risks with several IRS offices. However, a commitment to cost, benefit and risk analysis is not documented in the group's short- and long-term priorities. The draft planning documentation that we were given by IRS makes no mention of where such analyses would be included in IRS's priorities.

Federal guidance directs agencies to assess the costs, benefits and risks of government systems. OMB provides guidance to agencies for conducting economic cost-benefit and cost-effectiveness assessments that promote efficient resource allocation through well-informed decision making.³⁹ Specifically, these assessments should consider different alternatives to meet program objectives along with a discussion of costs and benefits. Further, OMB and NIST provide guidance for agencies to review new and existing electronic transactions to ensure that authentication processes provide the appropriate level of assurance.⁴⁰ Agencies can determine the appropriate level of assurance by conducting an assessment, mapping identified risks to the applicable assurance level, and selecting technology based on e-authentication technical guidance, among other steps. While we recognize that developing quantitative cost, benefit and risk estimates can be challenging or may not always be possible, qualitative analysis can also be informative, as discussed by OMB guidance.

Without analysis of costs, benefits and risks, IRS and Congress will not have quantitative information that could inform decisions about whether and how much to invest in the various authentication options. These decisions could include which authentication options to pursue (e.g., expanding the IP PIN or issuing a credential), where in the tax filing process authentication would be required (e.g., at the time of filing or after a return is flagged by IDT filters), and what level of assurance would be required (as detailed in OMB and NIST guidance).⁴¹ Cost, benefit and risk estimates for authentication would have the additional benefit of allowing comparisons with other options for combating IDT refund fraud, such as pre-refund W-2 matching. Both approaches could have significant costs for taxpayers and IRS, so more information about the tradeoffs would help inform IRS and congressional decision making.

³⁹OMB Circular A-94.

⁴⁰OMB M-04-04 and NIST Special Publication 800-63-2. OMB and NIST 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 two-factor authentication (e.g., a username and password plus a token displaying a new PIN every minute).

⁴¹OMB M-04-04 and NIST 800-63-2.

Conclusions

IDT refund fraud is a large, continually evolving threat that is costing taxpayers billions of dollars per year. Honest taxpayers who have had fraudulent tax returns filed in their name have the burden of proving to IRS who they are and waiting for delayed refunds. IRS has poured resources into trying to clean up the tax accounts of the honest victims and is playing a losing game of “pay and chase” with the thieves. A strategy that avoids these costs would be one to prevent fraudulent refunds from being issued in the first place. While IRS has a variety of preventive measures in place, the *Taxonomy* estimates show that additional preventative efforts could have significant benefits.

IRS’s *Taxonomy* estimates are one part of improving IRS’s prevention strategies. Because the *Taxonomy* helps IRS understand how and to what extent IDT refund fraud is evading IRS defenses, it can focus attention on where the risk is greatest and can help improve the design of IRS’s IDT filters. To reap the most benefit from the *Taxonomy*, decision makers—both IRS managers and Congress—need to understand how reliable the estimates are. Given the difficulties in estimating refund fraud, reporting only point estimates risks misleading decision makers about the extent and nature of IDT refund fraud. While a point estimate might lead to one decision, a range that reflects the uncertainty may lead decision makers to a different decision.

We previously recommended that IRS develop cost-benefit information on pre-refund W-2 matching, which IRS has committed to implementing. Another tool that IRS is beginning to implement is device identification, which has potential benefits at low costs. IRS has limited information about the costs, benefits and risks of a third option, taxpayer authentication. The lack of this information could hinder decision makers’ ability to select which option (or combination of options) is most cost beneficial.

Recommendations

To improve the reliability of *Taxonomy* estimates for future filing seasons, the Commissioner of Internal Revenue should follow relevant best practices outlined in the *GAO Cost Guide* by taking the following two actions:

- Documenting the underlying analysis justifying cost-influencing assumptions, and
- Reporting the inherent imprecision and uncertainty of the estimates. For example, IRS could provide a range of values for its *Taxonomy* estimates.

To ensure relevant information is available to decision makers, we recommend that the Commissioner of Internal Revenue estimate and document the costs, benefits and risks of possible options for taxpayer authentication, in accordance with OMB and NIST guidance.

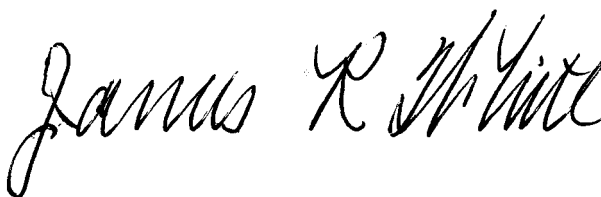
Agency Comments and Our Evaluation

We provided a draft of this product to the Commissioner of Internal Revenue for review and comment. In written comments, reproduced in appendix IV, IRS agreed with our recommendations. With regard to our first recommendation, IRS stated that it will follow best practices in the *GAO Cost Guide* for documenting the rationale supporting assumptions used in the *Taxonomy* estimates. IRS also stated that it will supplement its revenue lost estimates by reporting the inherent imprecision and uncertainty of estimates, subject to the availability of data and resources.

While we acknowledged IRS's resource limitations in the report, we also stated that reporting a point estimate without a range or some other indication of uncertainty could provide a false sense of precision about refunds prevented and paid. This false sense of precision could affect decisions about how to allocate resources to combat IDT refund fraud. Given the importance of these estimates, providing the proper context is also important. With regard to our second recommendation, IRS stated that its authentication group will develop a repeatable process to estimate and document the costs, benefits and risks of possible options for taxpayer authentication, in accordance with OMB and NIST guidance. However, the scope and analysis may be limited due to available resources and time. IRS also provided technical comments on figure 1, which we revised to acknowledge that the examples provided are for IDT refund fraud cases detected after refund issuance.

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. 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 whitej@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 V.

A handwritten signature in black ink that reads "James R. White". The signature is written in a cursive style with a large initial "J" and "W".

James R. White
Director, Tax Issues
Strategic Issues

Appendix I: Objectives, Scope, and Methodology

This report assesses (1) the quality of the Internal Revenue Service (IRS) *Identity Theft Taxonomy's (Taxonomy)* estimates of the cost of identity theft (IDT) refund fraud, and (2) IRS's progress in developing processes to track device identification numbers and to enhance taxpayer authentication.¹ The report discusses IDT refund fraud and not employment fraud.

To assess the quality of the *Taxonomy's* estimates of IDT refund fraud, we reviewed the *Taxonomy's* methodology and estimates for filing season 2013 and 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 (see text box).² In addition, 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, cost experts then considered best practices for the development of reliable cost estimates.

Selected Best Practices in Cost Estimating

Objective, reliable cost estimates

- Include all relevant costs.
- Document all cost-influencing ground rules and assumptions.
- Capture the source data used.
- Describe in sufficient detail the calculations performed and the estimating methodology used to derive each element's cost.
- Describe step by step how the estimate was developed so that a cost analyst

¹Device identification is the unique number associated with an individual device, such as a laptop computer, used to electronically file a return.

²GAO, *GAO Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs*, [GAO-09-3SP](#) (Washington, D.C.: March 2009) and OMB, *Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies*, (Washington, D.C.: October 2001), accessed September 25, 2014, http://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.

- unfamiliar with the program can understand what was done and replicate it.
- Provide evidence that the cost estimate was reviewed and accepted by management.
 - Are regularly updated to reflect significant changes in the methodology.
 - Contain few mistakes.
 - Include a sensitivity analysis.
 - Include a risk and uncertainty analysis.
 - Are not overly conservative or optimistic, but are based on an assessment of most likely costs.

Source: GAO Cost Estimating and Assessment Guide, GAO-09-3SP. | GAO-15-119

During our assessment of the *Taxonomy*, we interviewed IRS officials to better understand IRS's methodology. We also discussed the *GAO Cost Guide's* best practices with IRS officials who generally agreed with their applicability to the *Taxonomy*. IRS officials said many of the best practices are relevant to the *Taxonomy*, but questioned the applicability of best practices related to sensitivity and uncertainty analyses. They also questioned whether the *Taxonomy* itself was a cost estimate. We consulted with our cost estimating experts and concluded that the *Taxonomy* is a cost estimate because it is IRS's estimate of the amount of revenue lost due to IDT refund fraud. Further, given the importance of the *Taxonomy* and the fact that changes in the assumptions IRS makes and includes in the estimates substantially affect results, we believe providing information about the uncertainty of the *Taxonomy* estimates is warranted (as discussed in more detail in the report).

To analyze IRS's *Taxonomy* against the best practices, we reviewed *Taxonomy* documentation, conducted manual data testing for obvious errors, compared underlying data to IRS's *Refund Fraud & Identity Theft Global Report*, and conducted numerous interviews with IRS officials to understand the methodology the IRS used to create estimates. We also confirmed *Taxonomy* components where we had data available to cross check. We developed an overall assessment rating for each best practice using the following definitions:

- **Not met.** IRS provided no evidence that satisfies any portion of the best practice.
- **Minimally met.** IRS provided evidence that satisfies a small portion of the best practice.
- **Partially met.** IRS provided evidence that satisfies 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.

To assess IRS's progress in developing processes to track device identification numbers and to enhance taxpayer authentication, we reviewed *Internal Revenue Manual* sections detailing IRS's Identity Protection Program and IRS documentation for several tools developed to combat IDT refund fraud. We also interviewed IRS officials to learn about these efforts. These included the Identity Protection Personal Identification Number, device identification, authentication group, and other efforts related to identity authentication. We compared IRS's authentication group's planning document to OMB's guidance on cost-benefit analyses, as well as OMB and the National Institute for Standards and Technology (NIST) guidance on assessing levels of assurance for taxpayer authentication.³ We interviewed NIST officials to better understand the methodology used in their cost-benefit analysis of a credential-based taxpayer authentication system and to gather input on the advantages and disadvantages of this type of system.

To learn about additional actions IRS could take to prevent IDT refund fraud, we interviewed associations representing software companies, return preparers, and financial institutions. To help ensure our analysis covered a variety of viewpoints, we selected a nonprobability sample of 18 associations and stakeholders with differing positions and characteristics, based on IRS documentation and suggestions, our prior work, and other information. For example, to select associations representing financial institutions, we considered (among other factors) the size and type of institutions they represented (e.g., large or small banks, credit unions, and prepaid debit card companies). Because we used a nonprobability sample, the views of these associations are not generalizable to all potential third parties.

³OMB, *E-Authentication Guidance for Federal Agencies*, M-04-04 (Washington, D.C.: Dec. 16, 2003); *Circular A-94: Guidelines and Discount Rates for Benefit Cost Analysis of Federal Programs* (Washington, D.C.: 1992); and NIST, *Electronic Authentication Guideline*, Special Publication 800-63-2, (August 2013).

Table 3: List of Third Parties Interviewed

Software and Analytics Companies	<ol style="list-style-type: none"> 1. Equifax 2. H&R Block^a 3. Intuit 4. LexisNexis 5. SAS
Tax Software and Return Preparer Associations and Advisory Committees	<ol style="list-style-type: none"> 6. American Coalition for Taxpayer Rights 7. American Institute of CPAs 8. Electronic Tax Administration Advisory Committee 9. Free File Alliance
Financial Institution and Payment Associations	<ol style="list-style-type: none"> 10. American Bankers Association 11. BITS^b 12. The Clearing House 13. Credit Union National Association^c 14. NACHA – The Electronic Payments Association 15. National Association of Federal Credit Unions 16. Network Branded Prepaid Card Association
Others	<ol style="list-style-type: none"> 17. Federation of Tax Administrators 18. National Taxpayer Advocate

Source: GAO. | GAO-15-119

^aAlso offers in-person tax preparation and banking services.

^bTechnology policy division of the Financial Services Roundtable. BITS is not an acronym. At one time, BITS stood for “Banking Industry Technology Secretariat.” However, with financial modernization and the emergence of integrated financial services companies, that term is no longer used.

^cProvided written comments.

When possible, we used a standard set of questions in interviewing these associations and summarized the results of the semistructured interviews. However, as needed, we also sought perspectives on additional questions tailored to these associations’ expertise and sought their opinions on key issues. To determine the feasibility of various options and the challenges of pursuing them, we then communicated with IRS offices including (1) Privacy, Government Liaison, and Disclosure; (2) Customer Accounts Services, and (3) Return Integrity and Correspondence Services.

We conducted this performance audit from August 2013 to January 2015 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: Summary of Tools to Combat Identity Theft Refund Fraud

The Internal Revenue Service (IRS) has developed multiple tools to combat identity theft (IDT) refund fraud. IDT detection occurs at three stages of the refund process: (1) before the IRS accepts tax returns, (2) during IRS's tax return processing, and (3) after IRS issues tax refunds to taxpayers (or fraudsters). IRS uses some of these tools currently, while others are under development or were recommended by one of our prior reports.¹ Table 4 describes each tool and its status.

Table 4: Overview of Current and Potential IRS Tools Used to Combat Identity Theft Refund Fraud, by Processing Stage

Processing Stage	Tool	Description	Status
Pre-acceptance	Identity Protection Personal Identification Number (IP PIN)	IRS provides single-use identification numbers to IDT victims who have confirmed their identities. IRS offered a limited IP PIN pilot in 2014. For details, see GAO-14-633 and GAO-13-132T .	Current program
	Automatic electronic filing (e-file) checks	IRS authenticates taxpayers during e-filing using self-select personal identification numbers (PINs), the prior year's adjusted gross income (AGI), and e-file PINs. <i>Self-select PINs</i> require taxpayers to provide their prior year's self-created PIN. <i>E-file PINs</i> require taxpayers to authenticate certain information, such as the taxpayer's name, Social Security number (SSN), date of birth, address, and filing status.	Current program
	Duplicate return reject	IRS automatically rejects returns that are e-filed using a given Taxpayer Identification Number (such as an SSN) when that SSN has been filed on a previously filed return. This prevents multiple fraudulent returns being filed with the same Taxpayer Identification Number. While IRS officials are aware of e-file rejects (including duplicate return rejects), they do not know if the rejects are due to IDT refund fraud or other reasons.	Current program
	Duplicate return reject for married filing jointly returns	IRS currently uses a manual process to detect fraudulent married filing jointly returns in cases where the same Taxpayer Identification Number (such as a SSN) has been listed on multiple returns with more than two different spousal SSNs. IRS is identifying ways to automate this process during the pre-acceptance stage, according to IRS officials.	Program in development

¹GAO, *Identity Theft: Additional Actions Could Help IRS Combat the Large, Evolving Threat of Refund Fraud*, [GAO-14-633](#) (Washington, D.C.: Aug. 20, 2014).

**Appendix II: Summary of Tools to Combat
Identity Theft Refund Fraud**

Processing Stage	Tool	Description	Status
	Identity credential	Credentials—consisting of passwords or tokens—enable taxpayers to actively confirm their identities through authentication questions. Credentials could be received from IRS or a third party, and could be used when filing taxes and conducting other transactions.	Potential authentication option
During Return Processing	Pre-refund Form W-2, <i>Wage and Tax Statement</i> (W-2) matching	IRS validates taxpayer-reported return information (e.g., wages and compensation) with employer-reported information by matching W-2 information to tax returns before issuing refunds. ^a	Program under consideration/related GAO recommendation ^b
	Identity theft and other fraud filters	Automated filters screen returns for characteristics of IDT (or other) fraud, or screen for clusters of returns with similar characteristics. For details, see GAO-14-633 and GAO-13-132T .	Current program
	Return Review Program (RRP)	An automated system that is intended to detect criminal and civil noncompliance through sophisticated models and analysis.	Program in development ^c
	Authentication questions ^d	IRS confirms the identities of taxpayers whose returns are selected by its identity theft and other fraud filters, or who participate in the IP PIN pilot. Authentication questions ask about personal information that only the taxpayer should know (e.g., Who is your mortgage lender? Which of the following is your previous address?)	Current program
	Identity theft indicators	IRS places markers on taxpayer accounts that denote IDT problems. Indicators speed resolution by making a taxpayer's IDT problems visible to all IRS personnel with account access. For details, see GAO-14-633 and GAO-13-132T .	Current program
	Manual pattern matching	During tax return processing, IRS analysts look for patterns of suspicious activity to determine if a return is fraudulent and requires screening.	Current program
	Device identification analysis	Analyzes the unique identification number associated with a device (e.g., computer, tablet) to identify fraudulent returns filed from the same device.	Program in development
	Risk-based authentication strategy	Taxpayer returns are screened against third-party databases to assess the risk that the identity has been stolen before IRS accepts the return for processing. High-risk returns would require the taxpayer to answer authentication questions to confirm his or her identity, whereas low-risk returns would be processed.	Potential authentication option
Post-refund	Third-party leads	<i>External Leads Program</i> - third parties (e.g., financial institutions or software companies) report suspected IDT refund fraud. <i>Opt-In Program</i> – financial institutions electronically reject suspicious refunds. For details on both programs, see GAO-14-633 .	Current program ^e
	Taxpayer alerts	A taxpayer notifies IRS of IDT (e.g., calls IRS because of a duplicate return reject, or responds to an IRS compliance notice). For details, see GAO-14-633 .	Current program

Appendix II: Summary of Tools to Combat Identity Theft Refund Fraud

Processing Stage	Tool	Description	Status
	Information return matching	IRS finds IDT refund fraud when it matches tax return data to information returns as part of the Automated Underreporter (AUR) program, which matches tax return data to information returns, such as Form W-2, <i>Wage and Tax Statement (W-2)</i> . The legitimate taxpayer may not be aware of a stolen identity until after receiving a notice indicating the income and/or payment information IRS has on file is missing or does not match the information reported on the tax return.	Current program

Source: GAO analysis of IRS information. | GAO-15-119.

Note: This table provides examples of IRS tools, but it is not an exhaustive list. Tools listed focus on IDT prevention and detection, but not IDT customer service or enforcement efforts.

^aCurrently, IRS cannot do such matching because employers' wage data are unavailable until months after IRS issues most refunds. To facilitate the use of W-2 information to help combat IDT refund fraud, the Department of the Treasury (Treasury) proposed to Congress that the W-2 deadlines be moved to January 31. We found that IRS had not fully assessed the impacts of this proposal. Treasury also requested authority to reduce the 250-return threshold for electronically filing information returns. Without this change, some employers' paper W-2s could not be available for IRS matching until much later in the year, due to the additional time needed to process paper forms. For details, see [GAO-14-633](#).

^bGAO recommended that IRS assess the benefits and costs of accelerating W-2 deadlines and provide information to Congress on (1) IRS systems and work processes that would need to be adjusted, (2) potential impacts on taxpayers, IRS, the Social Security Administration, and third parties; and (3) any other changes that may be needed. In November 2014, IRS reported that it had convened an internal working group to address our recommendations and that it anticipated implementing our recommendations by July 2015. In addition, GAO suggested that Congress should consider providing the Secretary of the Treasury with the regulatory authority to lower the threshold for electronic filing of W-2s from 250 returns annually to between 5 and 10 returns, as appropriate. For details, see [GAO-14-633](#).

^cIRS officials told us that the next version of RRP is on a "strategic pause" while IRS officials clarify functionality amidst budget constraints. However, IRS piloted one component to detect IDT refund fraud for some filing season 2014 returns, and it plans to use this system in filing season 2015.

^dAuthentication questions are also known as "knowledge-based authentication questions" or "out of wallet" questions.

^eRelated to this, GAO recommended that IRS (1) provide aggregated information on the success of external party leads in identifying suspicious returns and emerging trends to relevant lead-generating third parties, and (2) develop a set of metrics to track external leads by the submitting third party. In November 2014, IRS reported that it is developing a reporting methodology and metrics to address our recommendations. For more information, see [GAO-14-633](#).

Appendix III: How Assumptions Affect *Identity Theft Taxonomy (Taxonomy)* Results – Two Examples

The Internal Revenue Service (IRS) developed the *Taxonomy* for a number of reasons, including the need to monitor both the volume and cost of identity theft (IDT) refund fraud attempts and the effectiveness of IDT defenses over time. *Taxonomy* estimates are based on IRS's administrative records of known IDT refund fraud (e.g., data on the number of duplicate returns). The *Taxonomy* also estimates IDT refunds by, for example, identifying returns with the characteristics of IDT refund fraud, as detected by the Automated Underreporter (AUR) program.¹

Best practices within the *GAO Cost Estimating and Assessment Guide* suggest that sensitivity and uncertainty analyses should be used to determine whether assumptions are potentially introducing error into an estimate.² The following examples demonstrate how the assumptions IRS makes (and includes in its estimates of IDT refund fraud) substantially affect *Taxonomy* results.

Example 1: IRS's Analysis Demonstrates that Assumptions Substantially Affect *Taxonomy* Estimates

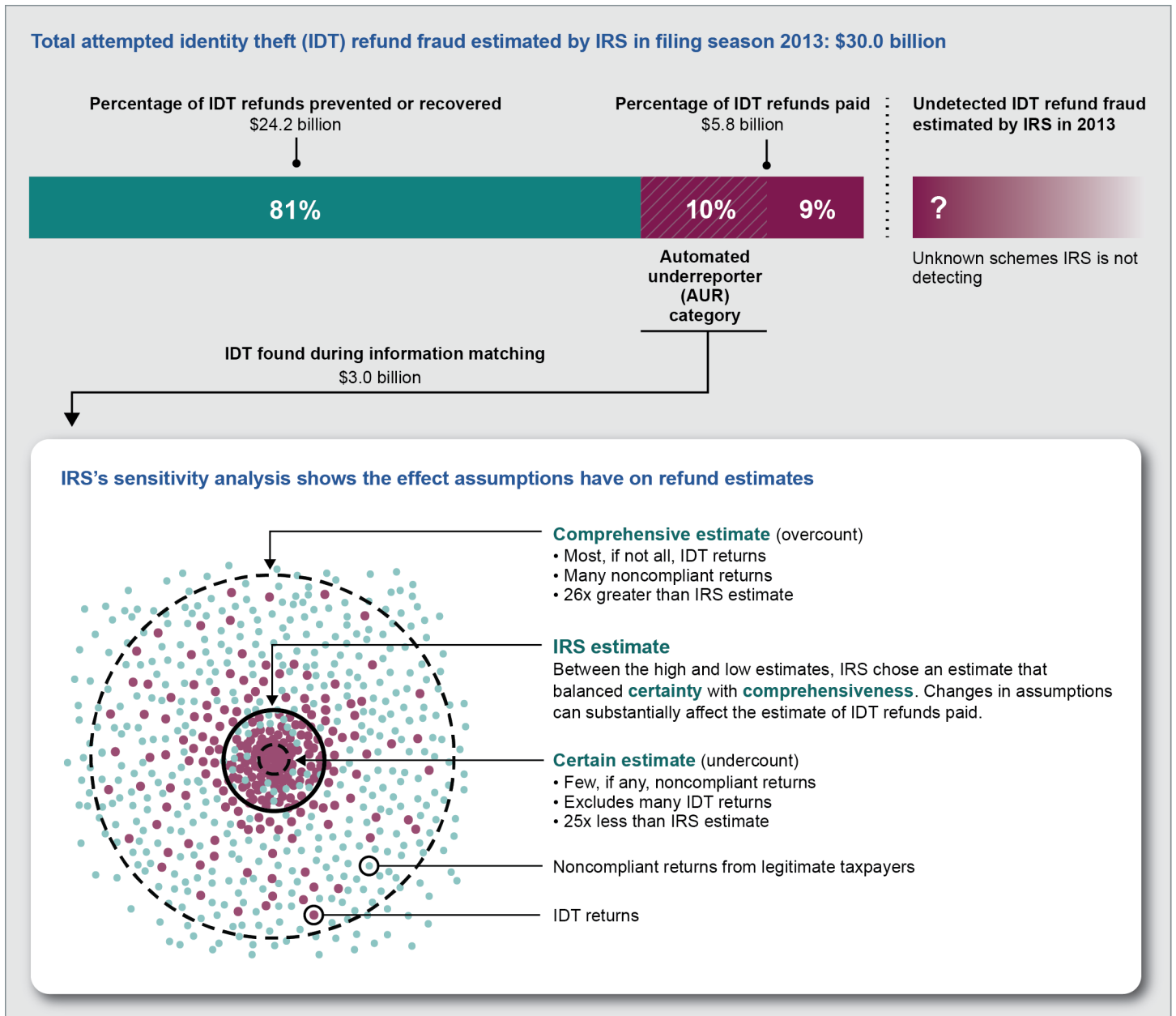
As shown in figure 4, \$3.0 billion of the estimated \$5.8 billion in IDT refunds paid in filing season 2013 are based on estimates developed using AUR data from information return matching (we refer to this part of the *Taxonomy* as the "AUR category"). To estimate the AUR category, IRS uses assumptions based on the characteristics of past IDT refund fraud. These characteristics enable IRS to identify which information return mismatches are IDT returns. IRS officials must develop assumptions about the IDT refund fraud characteristics because without conducting a tax return audit, it is impossible for officials to determine whether mismatches are IDT or are some other type of noncompliant return (i.e., a legitimate taxpayer makes a mistake or purposely files a noncompliant return). As IRS develops its assumptions, it uses them to help estimate which information return mismatches are noncompliant

¹The AUR program matches information returns (such as Form W-2, *Wage and Tax Statement*) to tax returns and pursues discrepancies after the filing season.

²A 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. 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. See *GAO Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs*, [GAO-09-3SP](#), (Washington, D.C.: March 2009).

returns (the turquoise dots in figure 4) and which are IDT returns (the purple dots).

Figure 4: How Assumptions Affect Taxonomy Estimates Based on Data from Information Return Matching



Source: GAO analysis of IRS data. | GAO-15-119

Appendix III: How Assumptions Affect Identity Theft Taxonomy (Taxonomy) Results – Two Examples

Note: The figure above is shown for illustrative purposes; the actual distribution of IDT versus noncompliant returns from legitimate taxpayers is unknown. To develop the magnitude measures above, we divided IRS's highest and lowest AUR category estimate by the estimate IRS chose in filing season 2013. Using these two extremes would likely result in too broad of a range in IDT refunds paid estimates.

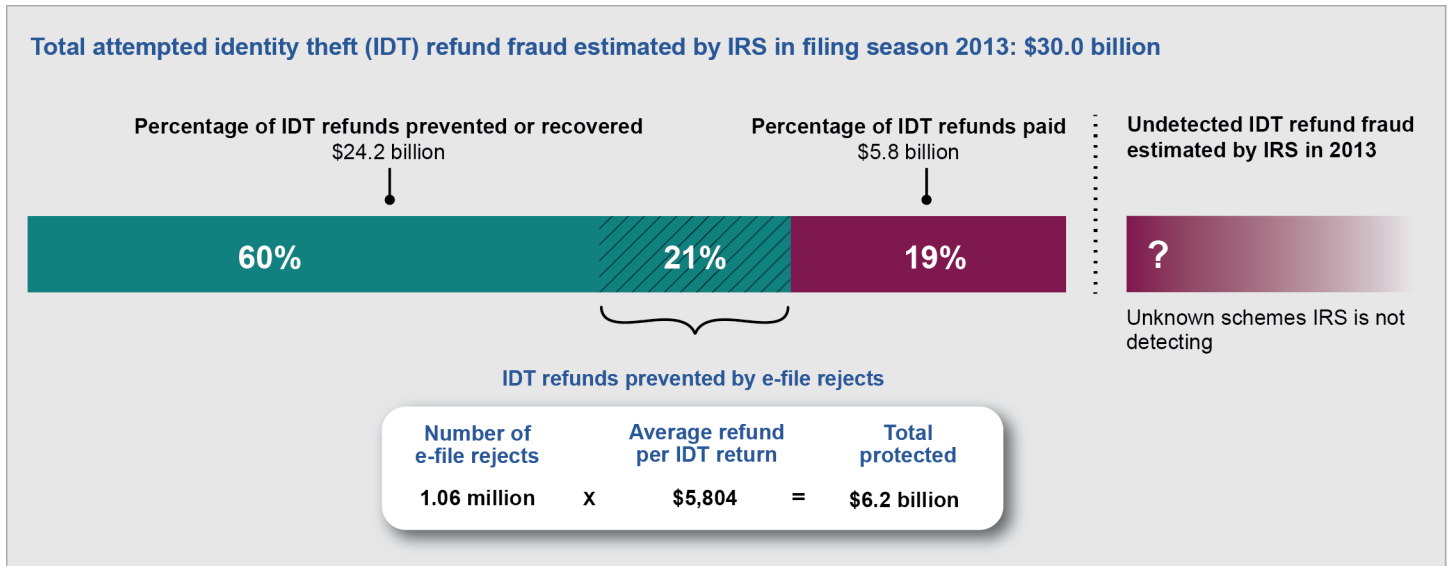
As further illustrated in figure 4, IRS chose assumptions that it believed best balanced comprehensiveness (that most IDT returns are likely included but legitimate returns are also included) with certainty (that many of the returns selected were IDT and include few, if any, legitimate returns). A completely comprehensive estimate (as illustrated by the larger circle) would be an overcount and could result in an IDT refund estimate about 26 times greater than IRS's current estimate, according to our analysis of the *Taxonomy*. In contrast, a completely certain estimate (as illustrated in the smaller circle) would be an undercount and would result in an IDT refund estimate that is 25 times less than IRS's current estimate. Using these two extremes would likely result in an "IDT refunds paid" estimate range that is too broad. Since IRS has not conducted an uncertainty analysis, we do not know the range that likely encompasses most cases of IDT.

Example 2: The *Taxonomy* Does Not Account for Variability in Refund Values

IRS uses an average refund value in certain *Taxonomy* categories, instead of using the actual value of each individual refund counted in the estimate. Therefore, it is likely that the total estimates of "IDT refunds paid" and "IDT refunds prevented" are imprecise. For example, figure 5 demonstrates how IRS developed its estimate of the value of refunds prevented by rejecting electronically filed returns (e-file reject).³ To develop its \$6.2 billion estimate, IRS multiplied the number of e-file rejects (1.06 million) by the average refund associated with IDT returns caught by IRS IDT filters and other fraud defenses (\$5,804).

³E-file rejects can occur, for example, when a return is electronically filed without an Identity Protection Personal Identification Number.

Figure 5: Estimating Refunds Prevented Using E-file Rejects and Average Refunds, Filing Season 2013



Source: GAO analysis of IRS data. | GAO-15-119

However, the average refund value of e-file returns detected by IRS IDT defenses can vary—indicating uncertainty in this estimate. For example, if IRS used the different average refunds in table 5 to develop its e-file reject estimate, the total could range from \$4.9 billion to \$8.7 billion.

Table 5: Potential Estimates of E-file Rejects Using Different IRS IDT Defenses, Calendar Year 2013

IDT defense	Average refund (in dollars per return)	Number of e-file rejects (in millions)	Total value of refunds prevented by e-file rejects (in billions)
Unpostable returns ^a	\$4,578	1.06	\$4.9
Identity theft filters (Dependent Database)	\$4,600	1.06	\$4.9
Returns detected as part of a repeat “Operation Mass Mail” scheme ^b	\$5,636	1.06	\$6.0
Fraud filters (Electronic Fraud Detection System)	\$7,422	1.06	\$7.9
Returns detected as part of a new “Operation Mass Mail” scheme ^b	\$8,235	1.06	\$8.7
IRS estimate using average refund value for all IDT defenses	\$5,804	1.06	\$6.2

Source: GAO analysis of IRS Refund Fraud and Identity Theft Global Report, December 2013. | GAO-15-119

^aReturns 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.

Appendix III: How Assumptions Affect Identity Theft Taxonomy (Taxonomy) Results – Two Examples

^bIRS 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.

Appendix IV: Comments from the Internal Revenue Service



DEPUTY COMMISSIONER

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

December 30, 2014

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

Dear Mr. White:

I have reviewed the draft report entitled *IDENTITY THEFT AND TAX FRAUD: Enhanced Authentication Could Combat Refund Fraud, but IRS Lacks an Estimate of Costs, Benefits, and Risks*, and appreciate your acknowledgment of the actions we have taken to improve our ability to define the scope of Identity Theft (IDT) refund fraud through the expanded use of data analytics. I also appreciate your acknowledgement of the challenges caused by the complexity and ever-evolving threat that IDT fraud presents. These challenges have been met during a period when the IRS incurred substantial reductions in funding while, concurrently, preparing for and implementing new major provisions of the Tax Code.

The IRS takes the threat of IDT refund fraud very seriously and is continually evaluating trends in IDT refund fraud and adjusting our processes to counteract new tactics employed by the identity thieves. Our detection models have become more dynamic, permitting us to make adjustments to address emerging threats in a more timely manner than was possible in the past. The IRS Identity Theft Taxonomy (Taxonomy) is an analytic process that helps inform our decisions in making adjustments to the fraud detection models, as well as assists in estimating the overall scope and impact of IDT refund fraud. It is important to note, regarding the examples of refund fraud detection illustrated in Figure 1 of the report, that the IRS stopped over \$17 billion dollars from being issued to identity thieves in 2013 (refunds blocked or stopped are not depicted in Step 3 of Figure 1 illustrations). The observations produced by the Taxonomy contributed to our ability to detect those returns and stop the fraudulent refunds during processing.

As the threat of identity theft has grown, the IRS has devoted resources to the development and implementation of preventive controls. As the prevalence of IDT refund fraud increased, return validation efforts evolved from simple error detection to a

2

widespread and robust evaluation of returns, drawing on a growing universe of data points and using elements of comparative analysis and predictive analytics. We continue to explore new strategies that will provide cost-effective solutions to deter attempts at IDT fraud, as well as to detect and stop it when attempted. As noted in the report, the IRS plans to collect unique device identification information when tax returns are filed electronically. This will provide additional data points to be considered by our fraud detection models, as well as provide valuable information to be used in the identification and prosecution of those persons perpetrating the fraud.

A taxpayer authentication process is another tool we are actively pursuing to supplement the existing Self-Select Personal Identification Number (PIN) and E-file PIN, to provide an additional layer of security in preventing IDT tax fraud. The IRS is evaluating many options in determining how we can best provide a method where returns can be filed with a reasonable assurance that the person filing the return is the legitimate owner of the Taxpayer Identification Number used on the return. As noted in the report, there are limitations associated with authentication processes that need to be considered before implementing taxpayer authentication on a wide scale. In some cases, IDT perpetrators may have access to the information that would be used in the authentication process. The challenge for tax administration is that identity thieves already have many pieces of information that are used for verifying identities in the private sector. If a Social Security Number has been compromised, there is a high probability the identity thief has also acquired the victim's name and address by virtue of the fact that those pieces of information are commonly recorded together. We have formed a team to explore the various options and make recommendations on how the IRS can best implement a widespread process for taxpayer authentication. We have also piloted a voluntary self-enrollment process for taxpayers residing in the states of Florida, Georgia, and the District of Columbia where individuals may proactively request an Identity Protection Personal Identification Number to be used when filing their tax returns. Based on our evaluation of the pilot, we intend to increase the size of the pilot population in 2015.

We agree that the costs, benefits, and risks of any program, process, or strategy must be evaluated to the greatest extent possible, although the depth and scope of this analysis may be limited based on available resources and time. In regards to IDT, there has been an urgency to act rapidly, especially given the ubiquity of personally identifiable information (PII) that has become available in the information age. Although victims of IDT refund fraud are made whole if a fraudulent refund is paid from their accounts; the loss is incurred by the United States Treasury and is a cost borne, collectively, by all U.S. taxpayers. Exposure to loss would have been significantly more than it has been if our actions had been delayed.

3

Responses to your specific recommendations are enclosed. If you have any questions, please contact Jodi L. Patterson, Director, Return Integrity and Compliance Services, Wage and Investment Division, at (404) 338-8961.

Sincerely,


John M. Dalrymple
Deputy Commissioner for
Services and Enforcement

Enclosure

Enclosure

Recommendations

RECOMMENDATION 1

To improve the reliability of *Taxonomy* estimates for future filing seasons, the Commissioner of Internal Revenue should follow relevant best practices outlined in GAO's *Cost Guide* by taking the following two actions:

- Documenting the underlying analysis justifying cost-influencing assumptions, and
- Reporting the inherent imprecision and uncertainty of the estimates. For example, IRS could provide a range of values for its *Taxonomy* estimates.

COMMENT

The IRS will follow best practices, as outlined in the "Ground Rules and Assumptions" section of the Government Accountability Office's (GAO) *Cost Assessment Guide; Best Practices for Estimating and Managing Program Costs*, in documenting the rationale supporting assumptions used in analyzing and determining the *Taxonomy* cost estimates.

The *Taxonomy* methodology uses point estimation in determining the amount of revenue protection from stopped refunds. The Global Identity Theft Report, which is a compilation of data from multiple sources within the IRS, provides underlying support to the *Taxonomy* estimates. The methodology for estimating revenue lost, attributable to refunds that were not stopped, relies on our knowledge of the Identity Theft profile. We will supplement our estimations of revenue lost by reporting the inherent imprecision and uncertainty of the estimates, subject to the availability of data and resources.

RECOMMENDATION 2

To ensure relevant information is available to decision makers, we recommend that the Commissioner of Internal Revenue estimate and document the costs, benefits and risks of possible options for taxpayer authentication, in accordance with OMB and NIST guidance.

COMMENT

The Authentication Group will incorporate GAO's recommendation into its standard operating procedures by developing a repeatable process to estimate and document the costs, benefits, and risks of possible options for taxpayer authentication, in accordance with OMB and NIST guidance although the depth and scope of that analysis may be limited based on available resources and time.

Appendix V: GAO Contact and Staff Acknowledgments

GAO Contact

James R. White, (202) 512-9110 or whitej@gao.gov.

Staff Acknowledgments

In addition to the individual named above, Neil Pinney, Assistant Director; Shannon Finnegan, Analyst-in-Charge; Dawn Bidne; Amy Bowser; Deirdre Duffy; Michele Fejfar; Timothy Guinane; Katharine Perl; Jason Lee; Donna Miller; Dae Park; Ellen Rominger; and Robyn Trotter made key contributions to this report. Gary Bianchi, Nina Crocker, Mary Evans, Ellen Grady, David Lewis, Paul Middleton, Sabine Paul, Sara Pelton, Bradley Roach, LaSonya Roberts, Susan Sato, and Julie Spetz also provided assistance.

Related GAO Products

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

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

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

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

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

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

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

GAO. 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](#). Visit GAO on the web at 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

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

Congressional Relations

Katherine Siggerud, Managing Director, 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, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

