



January 2020

IDENTITY THEFT

IRS Needs to Better Assess the Risks of Refund Fraud on Business-Related Returns

GAO Highlights

Highlights of [GAO-20-174](#), a report to the Chairman, Committee on Finance, U.S. Senate

Why GAO Did This Study

Business IDT is an evolving threat to both taxpayers and IRS and if not addressed can result in large financial losses to the government. The risk of business IDT has increased due to the availability of personally identifiable information and general ease of obtaining business-related information online. This makes it more difficult for IRS to distinguish legitimate taxpayers from fraudsters.

GAO was asked to review IRS's efforts to combat business IDT. This report (1) describes IRS's current efforts to detect business IDT, (2) evaluates IRS's efforts to prevent business IDT against selected fraud risk management leading practices, and (3) assesses IRS's efforts to resolve business IDT cases.

GAO reviewed IRS documents and business IDT fraud detection data, evaluated IRS's efforts to combat business IDT against two components of GAO's *Fraud Risk Framework*, analyzed case resolution data, and interviewed IRS officials.

What GAO Recommends

GAO is making six recommendations, including that IRS designate a dedicated entity to manage its business IDT efforts, develop a fraud risk profile consistent with leading practices, implement additional fraud filters consistent with the profile, and establish customer service-oriented performance goals for resolving business IDT cases. IRS agreed with five recommendations. IRS neither agreed nor disagreed with our recommendation to establish customer service-oriented performance goals, but stated it would take actions consistent with the recommendation.

View [GAO-20-174](#). For more information, contact James R. McTigue, Jr. at (202) 512-9110 or mctiguej@gao.gov.

January 2020

IDENTITY THEFT

IRS Needs to Better Assess the Risks of Refund Fraud on Business-Related Returns

What GAO Found

The Internal Revenue Service (IRS) has efforts in place to detect business identity theft refund fraud (business IDT), which occurs when thieves create, use, or try to use a business's identifying information to claim a refund. IRS uses computerized checks, or fraud filters, to screen incoming returns. From January 2017 to August 2019, IRS researched about 182,700 returns stopped by business IDT fraud filters. IRS determined that about 77 percent of returns (claiming \$38.3 billion) were not business IDT and about 4 percent of returns (claiming \$384 million) were confirmed business IDT. As of August 2019, IRS was reviewing the remaining returns.

The Fraud Reduction and Data Analytics Act of 2015 created requirements for agencies to establish financial and administrative controls for managing fraud risks. These requirements are aligned with leading practices outlined in GAO's *A Framework for Managing Fraud Risks in Federal Programs (Fraud Risk Framework)*. IRS has taken steps to understand fraud risks associated with business IDT but has not aligned its efforts with selected components within the *Fraud Risk Framework*. First, IRS leadership has demonstrated a commitment to identifying and combating overall identity theft refund fraud, but has not designated a dedicated entity to design and oversee business IDT fraud risk management efforts agency-wide. This is because the program is relatively new. Without designating an entity to help guide agency-wide business IDT fraud risk efforts, it is not clear which entity would be responsible for assessing business IDT risks and documenting the results.

Second, IRS has not conducted a fraud risk assessment or developed a fraud risk profile for business IDT consistent with the *Fraud Risk Framework's* leading practices. Doing so would help IRS determine the likelihood and impact of risks, the level of risk IRS is willing to tolerate, and the suitability, costs, and benefits of existing fraud risk controls. IRS officials stated that they have not formally performed a fraud risk assessment or developed a risk profile because they have directed their resources toward identifying and addressing business IDT that is occurring right now and improving fraud detection efforts. Documenting a risk profile would also help IRS determine whether additional fraud controls are needed and whether to make adjustments to existing controls.

Third, IRS has not assessed which business-related tax forms or fraud scenarios pose the greatest risk to IRS and taxpayers. Current business IDT fraud filters cover the most commonly filed tax forms; however, IRS has not developed fraud filters for at least 25 additional business-related forms that may be susceptible to business IDT. Without additional data on business IDT, IRS cannot estimate the full size and scope of this problem.

IRS has procedures for resolving business IDT cases and has described general guidelines for resolving business IDT cases, but it does not resolve all cases within these guidelines. Further, IRS has not established customer service-oriented performance goals for resolving business IDT cases, which is inconsistent with federal guidance. Establishing performance goals may help IRS better serve taxpayers and minimize additional costs to the Treasury.

Contents

Letter		1
	Background	5
	IRS Uses Fraud Filters and Collaborates with External Partners to Detect Business IDT	11
	IRS Has Taken Some Steps to Identify Business IDT Risks, but Efforts Are Not Fully Aligned with Selected Fraud Risk Management Leading Practices	13
	IRS Has Procedures for Resolving Business IDT Cases, but Has Not Established Customer Service-Oriented Performance Goals	25
	Conclusions	32
	Recommendations for Executive Action	33
	Agency Comments and Our Evaluation	34
Appendix I	Objectives, Scope, and Methodology	37
Appendix II	Comments from the Internal Revenue Service	44
Appendix III	GAO Contact and Acknowledgments	49
Table		
	Table 1: Examples of Business Types, Associated Tax Forms, and Related Information, 2018	6
Figures		
	Figure 1: Scenario of a Fraudster Committing Business Identity Theft by Obtaining a Business's Information	8
	Figure 2: Fraud Risk Management Framework	10
	Figure 3: Key Elements of the Fraud Risk Assessment Process	17
	Figure 4: About 87 Percent of IRS Pre-Refund Business Identity Theft (IDT) Cases Were Not Resolved within 90 Days, Cases Opened from Mid-January 2017 through December 2018	27
	Figure 5: About 17 Percent of IRS Post-Refund Business Identity Theft (IDT) Cases Were Not Resolved within 6 Months, Cases Opened July 2016 through December 2018	30

Abbreviations

AM	Accounts Management
BMFIC	Business Master File Identity Check
business IDT	business identity theft refund fraud
CI	Criminal Investigation
CIS	Correspondence Imaging System
DDb	Dependent Database
EIN	Employer Identification Number
Form 1120	<i>Form 1120, U.S. Corporation Income Tax Return</i>
Form 1120-S	<i>Form 1120-S, U.S. Income Tax Return for an S Corporation</i>
<i>Fraud Risk Framework</i>	<i>A Framework for Managing Fraud Risks in Federal Programs</i>
FRDAA	Fraud Reduction and Data Analytics Act of 2015
IDT	identity theft
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
OMB	Office of Management and Budget
PII	personally identifiable information
RAAS	Office of Research, Applied Analytics, and Statistics
RICS	Return Integrity and Compliance Services
RRP	Return Review Program
<i>Taxonomy</i>	<i>IRS Identity Theft Taxonomy</i>
TIGTA	Treasury Inspector General for Tax Administration

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 30, 2020

The Honorable Charles E. Grassley
Chairman
Committee on Finance
United States Senate

Dear Mr. Chairman:

Businesses of any size can be unsuspecting victims of tax fraud schemes, including business identity theft refund fraud (business IDT).¹ According to the Internal Revenue Service (IRS), business IDT occurs when thieves create, use, or try to use a business's identifying information—such as an Employer Identification Number (EIN)—in an attempt to claim a tax refund.²

IRS has recognized business IDT as a growing threat. IRS has reported that identity thieves show a sophisticated knowledge of the tax code and filing practices as they attempt to obtain valuable data that enable them to file fraudulent returns with potentially large refunds. In April 2019, IRS reported a 10 percent increase in the number of businesses notifying IRS that they have been victims of business IDT (2,233 notifications in 2017 to 2,450 in 2018).³ In addition to costing the government money, business IDT can hurt a business's reputation and credit and make a business more susceptible to other types of financial fraud.

IRS has noted that both businesses and individuals can suffer significant financial, social, and emotional hardship as victims of identity theft (IDT) refund fraud. As we have reported previously, the risk of IDT refund fraud has increased as personally identifiable information (PII) has become

¹In this report, business IDT refers to the fraudulent use of both business and employment tax forms. Both of these types of forms require an Employer Identification Number when filing with IRS, and a fraudster can file these forms to obtain a refund. In contrast, employment fraud occurs when an identity thief uses a taxpayer's name and Social Security number to obtain a job. GAO has an ongoing review of employment-related identity fraud and expects to issue a report on the result in early 2020.

²The EIN is a unique nine-digit number that IRS assigns to a business for tax purposes.

³Note that these counts only represent instances of business IDT where the taxpayer notified IRS. These counts would not include, for example, cases where an EIN is stolen and the taxpayer is unaware it is being used to file fraudulent tax returns.

more readily available through cyberattacks and data breaches.⁴ Businesses are further at risk of IDT refund fraud because their information is often easy to obtain, as they may post key information online, such as the names of corporate officers, address, and number of employees. Additional business information can also be obtained through online commercial databases. Further, federal regulations require some types of businesses to file public reports that include data which could be useful to a fraudster, such as data from annual financial statements. The availability of both PII and business information poses a threat to the tax system, making it more difficult for IRS to distinguish legitimate taxpayers from fraudsters.

Within this context, you asked us to examine IRS's efforts to detect, prevent, and resolve business IDT. This report (1) describes IRS's efforts to detect business IDT, (2) evaluates the extent to which IRS's efforts to prevent business IDT are consistent with selected fraud risk management leading practices, and (3) assesses IRS's efforts to resolve business IDT cases.

To address all of our objectives, we reviewed our prior reports on individual IDT refund fraud and the Treasury Inspector General for Tax Administration's (TIGTA) prior reports on business IDT. We also interviewed IRS officials from business units responsible for detecting, preventing, and resolving business IDT cases, specifically from Return Integrity and Compliance Services (RICS), Accounts Management (AM), and Criminal Investigation (CI). In December 2018, we visited IRS's campus in Ogden, Utah, to interview officials responsible for IRS's business IDT efforts and to observe how RICS and AM staff process and research business IDT cases using IRS information technology systems and tools.

To describe IRS's current efforts to detect business IDT refund fraud, we reviewed documentation describing the business IDT fraud filters IRS implemented from 2017 through 2019. We also analyzed data from IRS's Dependent Database (DDb) on business IDT fraud filter results, and data from the Business Master File Identity Check (BMFIC) case management system for applicable returns IRS received from mid-January 2017

⁴GAO, *Identity Theft: IRS Needs to Strengthen Taxpayer Authentication Efforts*, [GAO-18-418](#) (Washington, D.C.: June 22, 2018) and *Identity Theft and Tax Fraud: IRS Needs to Update Its Risk Assessment for the Taxpayer Protection Program*, [GAO-16-508](#) (Washington, D.C.: May 24, 2016).

through mid-August 2019. This was the most recent, complete, and available set of data at the time of our review. We tested key data elements, including computerized checks for missing, out-of-range, or logically inaccurate data, and interviewed officials knowledgeable about the data to discuss any limitations.

We determined that these data were sufficiently reliable to describe the volume of incoming returns stopped by business IDT fraud filters, associated refunds, and the outcome of business IDT cases. We also reviewed documentation and interviewed officials to understand IRS's efforts to collaborate with external partners to detect and prevent business IDT.

To evaluate the extent to which IRS's efforts to prevent business IDT are consistent with selected fraud risk management leading practices, we reviewed the Fraud Reduction and Data Analytics Act of 2015 (FRDAA) and *A Framework for Managing Fraud Risks in Federal Programs (Fraud Risk Framework)*.⁵ We generally focused our review on the first two components of the *Fraud Risk Framework*: (1) commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management, and (2) plan regular fraud risk assessments and assess risks to determine a fraud risk profile.⁶ In doing so, we reviewed agency strategic planning documents, organizational charts, and interviewed IRS officials to understand each business unit's respective role in detecting, preventing, and resolving business IDT.

We reviewed documentation on IRS's efforts to identify and assess business IDT fraud risks, relevant Internal Revenue Manual (IRM) sections, and prior GAO, TIGTA, and National Taxpayer Advocate reports

⁵Pub. L. No. 114-186, § 3, 130 Stat. 546 (2016). The Fraud Reduction and Data Analytics Act of 2015 requires OMB to establish guidelines that incorporate the leading practices of GAO's *Fraud Risk Framework*. The act also requires federal agencies to submit to Congress a progress report each year, for 3 consecutive years, on implementation of the risk management and internal controls established under the OMB guidelines. See GAO, *A Framework for Managing Fraud Risks in Federal Programs*, [GAO-15-593SP](#) (Washington, D.C.: July 28, 2015).

⁶The other components of the *Fraud Risk Framework* are: (3) design and implement a strategy with specific control activities to mitigate assessed risks and collaborate to ensure effective implementation; and (4) evaluate outcomes using a risk-based approach and adapt activities to improve fraud risk management. We did not assess IRS's business IDT efforts against these components of the *Fraud Risk Framework* given that IRS has not yet addressed the first two components.

related to three inherent fraud risks to business IDT. Additionally, we obtained information from interviews with RICS, AM, CI, RAAS, and IRS's Office of the Chief Risk Officer to understand IRS's efforts to combat business IDT through fraud risk management. We also reviewed documents and information on IRS's efforts to collect quality data on incoming business and employment returns. We compared these efforts to *Standards for Internal Control in the Federal Government* related to using quality information and leading practices identified in the *Fraud Risk Framework*.⁷

To assess IRS's current efforts to resolve business IDT cases, we reviewed IRS procedures for managing, researching, and resolving business IDT cases. We analyzed data from BMFIC and IRS's Correspondence Imaging System (CIS) to determine how long RICS and AM took to resolve business IDT cases. We assessed the reliability of CIS data by testing key data elements and interviewing knowledgeable IRS officials. Based on this effort and our assessment of BMFIC data reliability described above, we determined that these data were sufficiently reliable to determine how long it took RICS and AM to resolve business IDT cases.

We also interviewed IRS officials to determine potential reasons for delays in resolving cases. Finally, we compared RICS and AM's efforts to resolve business IDT cases against Office of Management and Budget (OMB) guidance on program management and providing customer service.⁸ See appendix I for details on our scope and methodology.

We conducted this performance audit from July 2018 to January 2020 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.

⁷GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 10, 2014).

⁸Office of Management and Budget, *Preparation, Submission and Execution of the Budget*, Circular No. A-11, pt. 6, § 270 (June 2019).

Background

Detecting IDT Refund Fraud Is Challenging

Over the past decade, our prior work has highlighted the evolving nature of individual IDT refund fraud and the challenges IRS faces in keeping up with fraudsters' tactics.⁹ Since 2015, our biennial High-Risk Report has highlighted the challenges associated with IDT refund fraud, the actions IRS needs to take to address them, and the cybersecurity issue of protecting PII amid large-scale data breaches.¹⁰ These challenges are relevant to business IDT and further compounded by the complexity of the business tax environment.

According to IRS officials, this complexity stems, in part, from the number of business types or structures, the various taxes that businesses pay, and the different tax forms businesses must file. Further, many businesses file tax returns throughout the year, unlike individual taxpayers who generally file income tax returns once a year. These factors make detecting, researching, and resolving potential business IDT cases more challenging than individual IDT cases.

When establishing a business, a business owner must determine the structure of the business for tax purposes, among other things, and may link business entities together in networks with multiple tiers.¹¹ In addition, unlike individuals, businesses are required to pay different types of taxes depending on the business structure. For example, C corporations and S

⁹For examples, see [GAO-18-418](#); [GAO-16-508](#); 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); and *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.: Sept. 8, 2009). Individual IDT refund fraud occurs when a fraudster obtains a person's identifying information, such as a Social Security number and date of birth, and uses it to file a fraudulent individual tax return.

¹⁰GAO, *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, [GAO-19-157SP](#) (Washington, D.C.: Mar. 6, 2019); *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, [GAO-17-317](#) (Washington, D.C.: Feb. 15, 2017) and *High-Risk Series: An Update*, [GAO-15-290](#) (Washington, D.C.: Feb. 11, 2015).

¹¹For additional information on multi-tiered business networks, see appendix II of GAO, *Partnerships and S Corporations: IRS Needs to Improve Information to Address Tax Noncompliance*, [GAO-14-453](#) (Washington, D.C.: May 14, 2014).

corporations pay income tax, and may also pay employment taxes and excise taxes on certain products and services such as fuel. Businesses are required to file different forms for each type of tax and may also file forms to claim various tax credits.¹² Table 1 provides examples of business types and associated tax forms, volume, and total refunds for fiscal year 2018.

Table 1: Examples of Business Types, Associated Tax Forms, and Related Information, 2018

Business type	Description	Primary business tax forms filed	Volume of IRS filings	Total refunds ^a
C Corporation	A legal entity that is separate from its shareholders, pays corporate income tax and other types of taxes, and distributes profits to shareholders. C corporations include most large, publicly held corporations.	Form 1120, <i>U.S. Corporation Income Tax Return</i>	2.1 million ^b	\$88.4 billion
S Corporation	A corporation that generally does not pay income taxes, but instead passes on income or losses to shareholders (who then must include that income or loss on their individual income tax returns). To be eligible to elect S corporation status, a corporation may not have more than 100 shareholders and may not have more than one class of stock, among other requirements.	Form 1120-S, <i>U.S. Income Tax Return for an S Corporation</i>	5.0 million	\$0.2 billion
Partnership	A business comprised of two or more individuals or entities (including corporations, trusts, estates, tax-exempt entities, and other partnerships). A partnership does not pay income tax but “passes through” any profits or losses to its partners (who then must include that income or loss on their individual income tax returns).	Form 1065, <i>U.S. Return of Partnership Income</i>	4.1 million	data not available ^c
Estates and Trusts	An estate is a taxable entity and a means to transfer assets from the decedent to beneficiaries. A trust is a relationship where one person holds a title to property, with an obligation to keep or use the property for the benefit of another person.	Form 1041, <i>U.S. Income Tax Return for Estates and Trusts</i>	3.1 million	\$8.8 billion
Total			14.3 million	At least \$97.4 billion^c

Source: GAO analysis of Internal Revenue Service (IRS) documents and data. | GAO-20-174

Notes: Volumes are rounded to the nearest hundred thousand; dollars are rounded to the nearest hundred million.

^aTax returns do not always involve a refund to the taxpayer.

^bIncludes data from the Form 1120 series except Form 1120-S, which is reported separately.

¹²Our review of IRS’s tax forms found that IRS Form 1120, *U.S. Corporation Income Tax Return* alone has 14 different variants depending on the type of corporation, and a total of 26 different schedules. In addition, various tax credits were available to businesses in 2018, including fuel tax credits and employment-related credits, though not all businesses are eligible for all tax credits.

⁹IRS's data source does not report partnership refund data since partnerships generally do not have a tax liability. Instead, any profits or losses are passed on to the underlying owners or shareholders, who include this information on their individual income tax returns.

IRS officials said that the complexity of the business tax environment makes it difficult for tax examiners to distinguish between true business IDT and frivolous tax arguments or noncompliance, such as incorrect or missing information on a form.¹³ Officials also noted that fraudsters may be attracted to the potential large payout associated with business tax refunds. According to IRS data, the average 2018 tax refund for corporations was about \$286,200 and about \$24,700 for estates and trusts.¹⁴ In contrast, the *IRS Data Book, 2018* reports that the average individual tax refund was about \$2,900.

Further, business IDT may also lead to other types of tax fraud. In addition to filing false business returns seeking a refund, fraudsters may use stolen EINs and business information to support an individual income tax refund scheme. For example, fraudsters may file fraudulent Forms W-2, *Wage and Tax Statement* with information on fictitious employees. These forms could then be used to file fraudulent individual tax returns seeking refunds.

Business IDT Can Occur in Two Ways

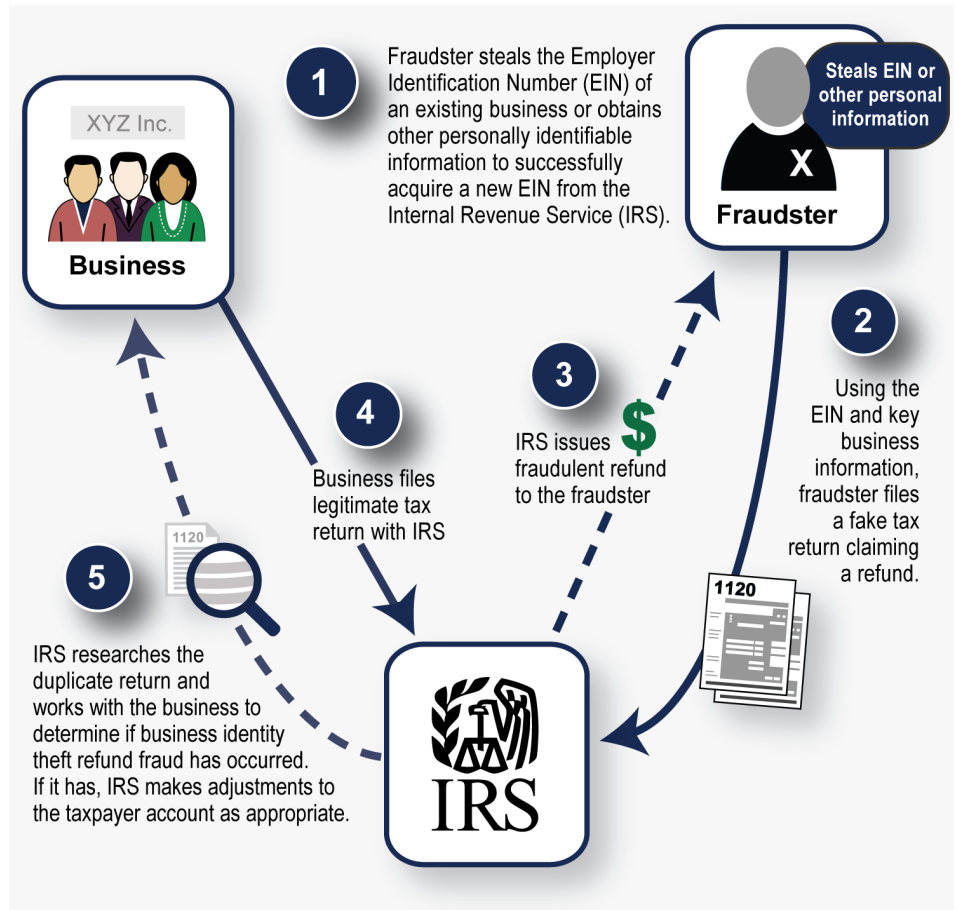
According to IRS, there are two ways a fraudster can commit business IDT, both of which involve the fraudulent use of the EIN.

1. **Obtain an existing EIN.** In this scenario, a fraudster obtains federal tax information from an existing business (see fig. 1). The business may be active or dormant, meaning that the business owner has not filed a tax return for at least two tax periods. The fraudster then uses the EIN and other key business information to file a fraudulent business return, such as Form 1120.
2. **Fabricate an EIN.** In this scenario, a fraudster steals the identifying information of an individual, such as a Social Security number and uses it to apply for an EIN. The fraudster would then use the fabricated EIN to complete and file false business returns.

¹³Taxpayers file returns with frivolous or unsupported tax arguments to avoid paying taxes or reduce their tax liability. According to IRS, an example of a frivolous tax argument includes stating that filing a tax return is voluntary. IRS can assess a \$5,000 penalty against persons submitting a frivolous submission. 26 U.S.C. § 6702

¹⁴The average corporate tax refund includes returns filed on the Form 1120 series.

Figure 1: Scenario of a Fraudster Committing Business Identity Theft by Obtaining a Business's Information



Source: GAO analysis of IRS documents. | GAO-20-174

Note: This is an illustrative example and does not apply to all business tax return filings.

Federal Agencies Are Required to Identify, Assess, and Manage Fraud Risks

In June 2016, Congress passed and the President signed into law the Fraud Reduction and Data Analytics Act of 2015 (FRDAA), which created requirements for agencies to establish financial and administrative controls for managing fraud risks.¹⁵ These requirements are aligned with leading practices outlined in our *Fraud Risk Framework*. In addition, guidance from OMB affirms that managers should adhere to the leading

¹⁵Pub. L. No. 114-186, 130 Stat. 546 (June 30, 2016).

practices identified in the framework.¹⁶ The *Fraud Risk Framework* provides key components and leading practices for agency managers to use when developing efforts to combat fraud in a strategic, risk-based way. The framework consists of four primary components of fraud risk management: commit, assess, design and implement, and evaluate and adapt, as shown in figure 2.

Specifically, the components call for agencies to (1) commit to combatting fraud by creating an organizational culture conducive to fraud risk management, (2) plan regular fraud risk assessments and assess risks to determine a fraud risk profile, (3) design and implement a strategy with specific control activities to mitigate assessed fraud risks, and (4) evaluate outcomes using a risk-based approach and adapt activities to improve fraud risk management.

¹⁶The act required OMB to establish guidelines that incorporate the leading practices of GAO's *Fraud Risk Framework*. Office of Management and Budget, *Management's Responsibility for Enterprise Risk Management and Internal Control*, Circular No. A-123 (Washington, D.C.: July 15, 2016).

Figure 2: Fraud Risk Management Framework



Source: GAO. | GAO-20-174

According to the *Fraud Risk Framework*, the four components are interdependent and mutually reinforcing. For example, fraud response efforts can inform preventive activities, such as using the results of investigations to enhance fraud detection efforts. We have previously reported that preventive activities generally offer the most cost-efficient use of resources, since they enable managers to avoid a costly and

inefficient “pay-and-chase” model.¹⁷ The framework also reflects ongoing activities for monitoring and feedback that apply to all four components.

IRS Uses Fraud Filters and Collaborates with External Partners to Detect Business IDT

IRS uses computerized checks, or fraud filters, to screen incoming tax returns for known or suspected characteristics of fraud. As of September 2019, IRS had implemented 19 unique fraud filters that assess incoming returns on certain business and employment tax forms.¹⁸ These fraud filters help IRS determine if an incoming return exhibits suspicious characteristics. IRS also cross-references these returns against lists of taxpayer identification numbers previously involved in data breaches and at greater risk of tax-related identity theft. IRS officials stated that they plan to implement additional fraud filters for three employment tax forms for the 2020 filing season.

Our analysis of IRS’s data shows that from January 2017 to August 2019, business IDT fraud filters stopped about 188,500 incoming business returns as potential IDT, claiming \$47.6 billion in refunds. Of these, IRS performed in-depth research on about 182,700 returns claiming \$47.3 billion in refunds. IRS determined that about 77 percent of these cases (140,100 cases) claiming \$38.3 billion in refunds were not business IDT while about 4 percent (7,900 cases) were confirmed business IDT claiming \$384 million in fraudulent refunds. The remaining cases were still under review as of August 2019.¹⁹ However, as we discuss later in this report, these estimates do not capture the full size and scope of business IDT.

¹⁷“Pay-and-chase” refers to the practice of detecting fraudulent transactions and attempting to recover funds after payments have been made. We have previously reported that implementing strong preventive controls can help defend against invalid payments, including tax refunds. GAO, *Improper Payments: Remaining Challenges and Strategies for Governmentwide Reduction Efforts*, [GAO-12-573T](#) (Washington, D.C.: Mar. 28, 2012).

¹⁸Most business IDT filters use the same logic for each form. For example, one filter checks if the individual responsible for the business has IDT indicators on their account. This same filter is run on the forms IRS currently screens for business IDT. IRS officials stated that they count fraud filters individually and have implemented a total of 58 filters for business tax forms and 22 filters for employment forms.

¹⁹As of August 2019, about 19 percent of total business IDT cases (34,700 cases) claiming \$8.7 billion in refunds were open or unresolved. About 87 percent of these cases were from returns filed in 2019.

In addition to developing fraud filters, IRS has established more advanced fraud detection efforts through the Return Review Program (RRP).²⁰ As of September 2019, IRS was developing and testing fraud detection models in RRP for certain business tax forms. IRS officials said they intend to develop additional models, such as those to address fuel tax credit fraud and entity fabrication. Officials also noted that they will continue to rely on fraud filters to detect potentially fraudulent business returns, even after expanding RRP's functionality.

Further, IRS's broader fraud detection efforts include working with external partners. For example, IRS collaborates with states and industry partners through the Security Summit Business IDT sub-workgroup.²¹ This group has identified business-related data elements that are captured during the tax filing process and analyzed for potential suspicious patterns that could indicate business IDT. During the 2018 filing season, IRS analyzed 37 data elements from incoming business tax returns and 10 data elements on incoming employment tax returns, including, for example, characteristics of the computer used to submit the return.²² IRS officials also stated that they are working directly with tax practitioners to help improve the quality of the data they collect to better inform future business IDT fraud filters and models.

In addition, in December 2017, IRS initiated a pilot project with the Alabama Department of Labor to help detect and prevent business IDT. IRS officials stated that they send the department a data extract on all newly issued EINs from the prior month. The state performs research on these businesses and, in turn, sends IRS a list of businesses that it has determined to be fraudulent. As a result, IRS is able to deactivate the fraudulent EINs before the fraudster files a false business, employment, or individual tax return claiming a refund. This allows IRS to reject returns

²⁰IRS detects and selects potentially fraudulent individual tax returns using RRP to prevent the issuance of invalid refunds. According to IRS, RRP uses advanced analytic techniques and evaluates data from various sources, including information from individual IDT fraud filters. See GAO, *Tax Fraud and Noncompliance: IRS Could Further Leverage the Return Review Program to Strengthen Tax Enforcement*, [GAO-18-544](#) (Washington, D.C.: July 24, 2018).

²¹In March 2015, IRS created the Security Summit with state tax administrators, tax preparation and software firms, and financial institutions to improve information sharing and collaboratively address critical issues such as IDT refund fraud.

²²In filing season 2018, the Security Summit collected data on certain incoming business and employment tax forms. Not all data elements were collected for each type of form.

associated with the fraudulent EINs. According to IRS data, in 2018 IRS identified about 3 percent (1,343 out of 53,826) of new EINs in Alabama as fraudulent. The early results of this collaborative effort indicate that this project shows promise, and IRS officials stated that they are working to determine if they can expand the initiative to other states.

IRS Has Taken Some Steps to Identify Business IDT Risks, but Efforts Are Not Fully Aligned with Selected Fraud Risk Management Leading Practices

IRS Has Developed an Organizational Culture to Help Combat Fraud, but Lacks a Designated Entity to Oversee Business IDT Efforts

One component of our *Fraud Risk Framework* calls for agencies to create an organizational culture conducive to combating fraud.²³ Such a culture can be created through “tone at the top,” whereby senior-level staff demonstrate commitment to integrity and combating fraud, and actions that involve all levels of the agency in setting an antifraud tone that permeates the organization. In addition, the *Fraud Risk Framework* calls for agencies to designate an entity to lead fraud risk management activities.

Commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management.



Among other things, the designated entity should have defined responsibilities and the necessary authority to perform its role, including managing a fraud risk assessment process and coordinating antifraud activities across the program. Our prior work has shown that when agencies formally designate an entity to design and oversee fraud risk management activities, their efforts can be more visible across the agency, particularly to executive leadership.²⁴

²³GAO-15-593SP.

²⁴For example, see GAO, *Medicare and Medicaid: CMS Needs to Fully Align Its Antifraud Efforts with the Fraud Risk Framework*, GAO-18-88 (Washington, D.C.: Dec. 5, 2017).

Consistent with the *Fraud Risk Framework*, IRS leadership has demonstrated a commitment to identifying and combating overall IDT refund fraud. For example, the agency has recognized the broad and evolving challenge of IDT refund fraud in its fiscal year 2018–2022 strategic plan. Also, as previously discussed, IRS has expanded its fraud detection activities to prevent payment of fraudulent refunds, including refunds on business-related returns.

In addition, our 2019 High-Risk Report noted that IRS took significant actions to facilitate information sharing with states and industry partners through the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center.²⁵ Further, IRS has implemented agency-wide antifraud efforts, including bringing officials together from across the organization to discuss potential fraud risks. These efforts have helped to foster an antifraud tone across IRS, according to IRS officials.

At the business unit level, four IRS entities have responsibility for detecting, preventing, and resolving business IDT, as described below. However, IRS has not designated a lead entity to design and oversee business IDT fraud risk management activities across the agency, including a fraud risk assessment, consistent with leading practices. During our interviews with IRS, we found that IRS officials were knowledgeable about the business IDT policies, processes, and outcomes in their individual unit. However, none of the entities has defined responsibilities and the necessary authority to manage fraud risk across the business units. Further, no one we spoke with could articulate an agency-wide view of the problem and its potential impact on IRS.

- Return Integrity and Compliance Services (RICS) is responsible for detecting potential fraud on incoming business tax returns during the “pre-refund” phase (i.e., the period from when IRS accepts the return but before it issues a refund). About 20 RICS and Integrity and Verification Operations tax examiners are responsible for researching taxpayer accounts to confirm whether or not business IDT occurred. Tax examiners are also responsible for resolving cases to both prevent IRS from paying out fraudulent refunds and ensure that legitimate taxpayers’ returns are released for processing. RICS refers cases to other IRS units if the case shows other signs of fraud, such as a frivolous return.

²⁵[GAO-19-157SP](#).

-
- Accounts Management (AM) is responsible for researching and resolving potential business IDT cases identified during the “post-refund” phase (i.e., after a refund has been paid). AM customer service representatives perform in-depth account research and work with taxpayers to determine if business IDT has occurred. In cases of confirmed business IDT, AM corrects related account errors and enters appropriate IDT markers on the taxpayer’s account. According to IRS officials, about five AM staff work on business IDT cases one day a week or as needed.
 - Criminal Investigation (CI) investigates large-scale tax schemes and other financial fraud, including fraud related to IDT.
 - Office of Research, Applied Analytics and Statistics (RAAS) is responsible for supporting RICS and other business units in identifying and developing various business IDT fraud detection capabilities. RAAS also performs analyses to help IRS determine how best to proceed with other fraud detection and prevention efforts.

IRS officials stated that representatives from the four business units meet regularly to share information on cases and discuss challenges. Further, IRS officials stated that the IDT Executive Steering Committee—which last met in October 2018—is responsible for providing general oversight and guidance to business units working on IDT-related efforts.²⁶ However, our review of several sets of Committee meeting minutes indicates that while RICS has briefed committee members on the status of various business IDT efforts, they have not specifically discussed business IDT program priorities, potential fraud risks, or resources.

When asked why IRS has not designated an entity to be responsible for overseeing business IDT fraud risk efforts, IRS officials said its business IDT efforts may not require additional oversight because they are significantly smaller than IRS’s individual IDT efforts in terms of both case volume and number of employees. They also said that the business IDT efforts are relatively new. However, with no more than 30 IRS employees working on business IDT issues, each business unit is mainly focused on day-to-day operations.

The absence of an entity to lead business IDT fraud risk efforts may contribute to the issues we identify later in this report related to identifying and assessing business IDT fraud risks consistent with leading practices

²⁶The IDT Executive Steering Committee was established in October 2012 and is comprised of senior executives from various business units within IRS.

and delays in resolving business IDT cases. The *Fraud Risk Framework's* leading practices provide flexibility in structuring the designated entity to best support an agency's fraud risk management efforts. For example, leading practices note that the designated entity could be an individual or a team, and can vary depending on factors like existing organizational structures and expertise within the agency.

In addition, employees across an agency or program, as well as external entities, can be responsible for the actual implementation of fraud controls. For example, IRS could designate one business unit as a lead entity, or leverage existing cooperative relationships between RICS, AM, CI, and RAAS to establish a business IDT leadership team with defined responsibilities and authority for managing fraud risk.

A lead entity could help provide a strategic direction, coordination across business units, and oversight for managing IRS's business IDT fraud risks. Further, without a designated entity, it is not clear which entity would be responsible for assessing business IDT risks and documenting the results, consistent with leading practices. These activities are important to combat the evolving threat of business IDT.

IRS Has Not Developed a Business IDT Fraud Risk Profile

IRS Has Not Developed a Fraud Risk Profile Based on Assessed Business IDT Risks

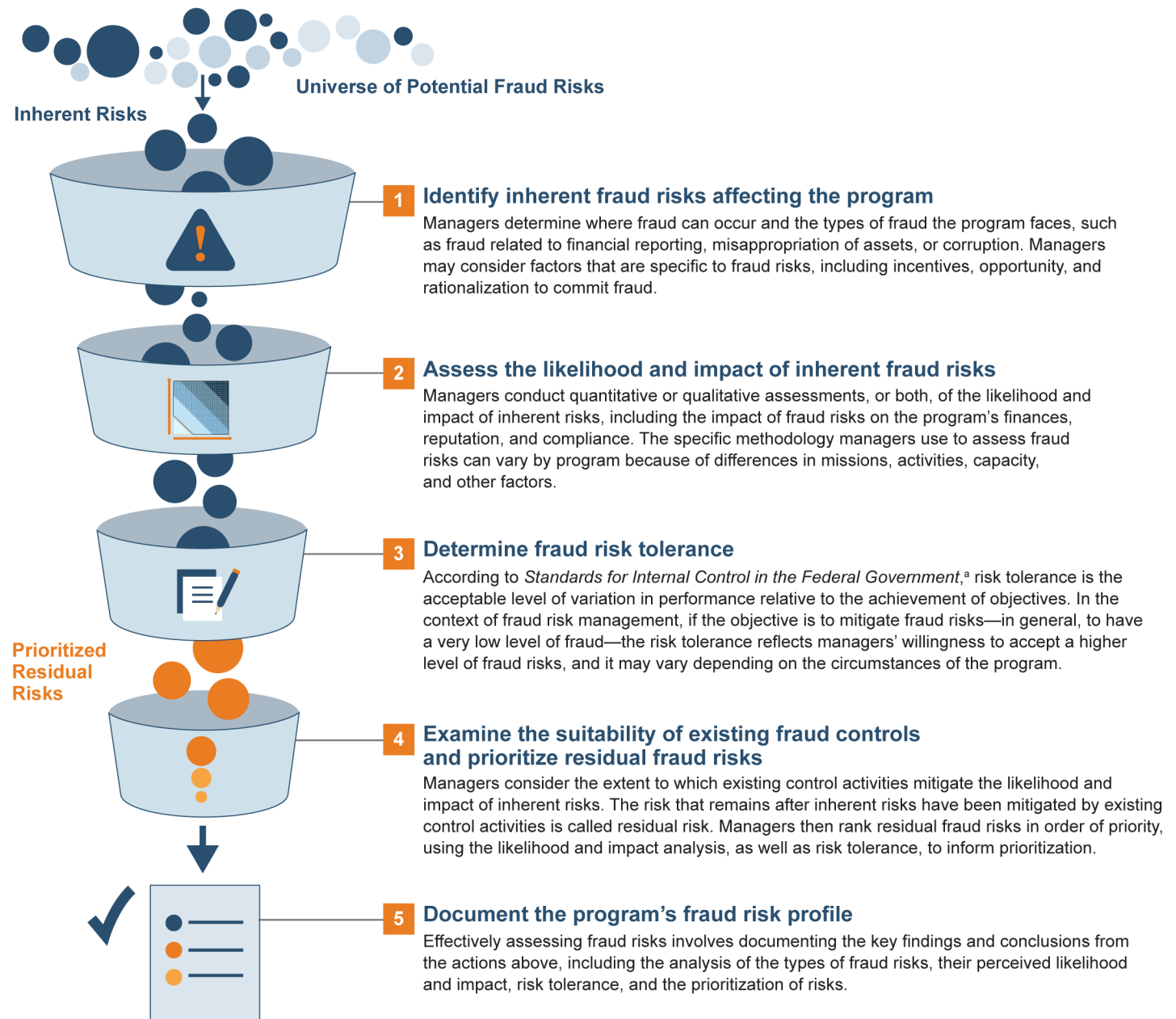
Plan regular fraud risk assessments and assess risks to determine the likelihood, impact, and level of acceptable risk.



The *Fraud Risk Framework* calls for agencies to regularly plan and perform fraud risk assessments to determine a risk profile. Fraud risk assessments that align with the *Fraud Risk Framework* involve (1) identifying inherent fraud risks affecting the program, (2) assessing the likelihood and impact of those fraud risks, (3) determining fraud risk tolerance, (4) examining the suitability of existing fraud controls and prioritizing residual fraud risks, and (5) documenting the results (see fig. 3).²⁷ Such a risk assessment provides the detailed information and insights needed to create a fraud risk profile, which, in turn, is the basis for creating an antifraud strategy for the program.

²⁷ According to federal standards for internal control, an inherent risk is “the risk to an entity prior to considering management’s response to the risk.” Inherent risks can exist due to the complex nature of an entity’s programs, policies, organizational structure, or the use of new technology in operational processes. Management’s lack of response to inherent risks can cause deficiencies in the internal control system. See [GAO-14-704G](#).

Figure 3: Key Elements of the Fraud Risk Assessment Process



Source: GAO. | GAO-20-174

^aGAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 10, 2014).

IRS has taken preliminary steps to understand fraud risks associated with business IDT through data analysis efforts and internal discussions with subject matter experts. However, IRS has not fully identified and assessed fraud risks to business IDT consistent with leading practices. These practices include identifying and assessing the likelihood of inherent fraud risks, determining a fraud risk tolerance, and examining the suitability of existing fraud controls to determine if they appropriately address identified risks.

IRS business units use current and prior year tax return data and information on known business IDT threats to improve existing fraud detection efforts and develop new efforts. For example, RICS and RAAS officials stated that they regularly collaborate to discuss the feasibility of new fraud filters and identify and prioritize analyses on business IDT data. This effort has resulted in IRS business units identifying 38 discrete projects to, for example, analyze existing fraud filter performance and understand business tax return filing behaviors. RICS officials stated they typically identify two to three projects to begin each year, resources permitting.

In addition, IRS officials stated that at the end of each filing season, they review and analyze confirmed business IDT cases to identify any new patterns or trends that may be useful for enhancing existing fraud filters and developing fraud detection models in RRP. Further, RAAS has performed ad hoc data analyses, such as on the characteristics of fabricated entities, to help understand potential risks to the business tax environment.

While these are positive steps, IRS has not assessed business IDT fraud risks consistent with leading practices in the *Fraud Risk Framework*. For example, IRS has not identified and documented inherent fraud risks in the business tax environment, or assessed the likelihood of their occurrence and impact on IRS—the first two steps of a fraud risk assessment process. Further, our review of past GAO, Treasury Inspector General for Tax Administration (TIGTA), and National Taxpayer Advocate reports identified issues that pose inherent risks to IRS's business IDT efforts. These risks include weaknesses with correspondence-based authentication, EIN vulnerabilities, and the high false detection rates for IDT fraud filters. We consider these to be inherent risks due to the complex nature of the business tax environment and IRS management's overall limited response to them.

Weaknesses with correspondence-based authentication. To help verify whether a suspicious business tax return is legitimate, IRS's business IDT procedures rely on correspondence-based authentication. This involves the taxpayer answering several brief, written questions about the business and sending this information to IRS via mail.²⁸ IRS officials stated that they believe correspondence-based authentication is no less secure than other forms of authentication, such as having business owners verify their identity in-person at a Taxpayer Assistance Center or authenticating via telephone.

However, unlike other forms of authentication, correspondence-based authentication is inherently less secure because it may not require the taxpayer to verify their identity using a government-issued form of identification. Consequently, IRS has less assurance that the person is the actual business owner and the return in question is legitimate.

In June 2018, we reported that IRS had not performed risk assessments to identify, assess, and mitigate risks associated with correspondence-based authentication because it did not have a policy that requires regular assessments and timely mitigation of identified issues.²⁹ Therefore, without a policy for conducting risk assessments for correspondence-based authentication and a plan for performing an assessment, IRS may underestimate known risks and overlook emerging threats to the tax environment. We recommended that IRS establish a policy for conducting such risk assessments and develop a plan for performing them. IRS agreed with our recommendations and, as of November 2019, had developed a draft policy for conducting risk assessments. However, IRS had not yet developed a plan for performing these assessments. IRS officials stated that they intend to address these recommendations by May 2020.

EIN vulnerabilities. In February 2018, TIGTA identified concerns with IRS's EIN application process and made 18 recommendations, including that IRS improve processes to ensure that the applicant meets the

²⁸IRS stated that multiple individuals may be authorized to act on behalf of a business. When attempting to authenticate a suspicious tax return, IRS will contact both the business itself and the responsible individuals by mail.

²⁹See [GAO-18-418](#). We also found that IRS had not performed risk assessments for its telephone and in-person authentication channels. We recommended that IRS establish a policy for conducting risk assessments for telephone and in-person authentication and to develop a plan for performing them.

requirements for obtaining an EIN and implement policies to help detect potential abuse of the online EIN application system.³⁰ IRS agreed with 15 of TIGTA's recommendations and, as of September 2019, IRS reported that it had addressed 11 recommendations. The four unaddressed recommendations aim to improve data collection and validation in the EIN system, which could help IRS identify suspicious applications. IRS officials stated that these improvements are on hold due to limited resources and competing priorities.

In addition, characteristics of the EIN may make it inherently risky and susceptible to fraudsters. According to IRS, a business's EIN is not considered PII and is not required to be protected like a Social Security number. This may make it easier for a fraudster to obtain an existing EIN and file a fraudulent business tax return. In addition, we have previously reported that fraudsters may target paid preparers, tax software providers, and other third parties to steal taxpayer data to commit IDT refund fraud or other types of financial crimes.³¹ These data may include existing EINs or the necessary information to obtain a new EIN, making it easier for fraudsters to file fake business returns.

IRS officials stated that they recognize the potential risk of the EIN application process, but must balance the needs of legitimate businesses against IRS's responsibility to detect and prevent fraud. Officials noted that they have security measures in place to detect potentially suspicious activity in the online EIN application and fraud filters to detect when taxpayers file a return with a dormant EIN. A fraud risk assessment consistent with leading practices would help IRS establish a risk tolerance for the EIN process and determine if its existing fraud controls are sufficient to address the vulnerabilities inherent to the EIN application process.

High false detection rates for IDT fraud filters. The National Taxpayer Advocate's 2018 *Annual Report to Congress* noted that one of IRS's most serious problems is a high false detection rate in its fraud detection

³⁰Treasury Inspector General for Tax Administration, *Actions Are Needed to Reduce the Risk of Fraudulent Use of Employer Identification Numbers and to Improve the Effectiveness of the Application Process*, 2018-40-013 (Washington, D.C.: Feb. 7, 2018).

³¹GAO, *Taxpayer Information: IRS Needs to Improve Oversight of Third-Party Cybersecurity Practices*, [GAO-19-340](#) (Washington, D.C.: May 9, 2019). These data include PII and other personal, financial, or federal tax data for individuals and businesses.

systems.³² In general, the false detection rate is the number of legitimate returns selected by the IRS as potentially fraudulent, divided by the total number of returns selected as potentially fraudulent. The National Taxpayer Advocate noted that IRS's false positive rate for individual IDT filters was 63 percent in 2018. The high rate contributed to increased processing times and delays in issuing refunds for legitimate returns. It also created additional work for IRS. Similarly, our data analysis of BMFIC data shows that IRS's business IDT fraud filters had about an 85 percent false detection rate for returns screened by fraud filters from mid-January 2017 to December 2018.³³

In September 2019, IRS officials described several factors contributing to the high false detection rate for business IDT fraud filters. These factors include taxpayers and tax preparers failing to update key information with IRS, cross-referenced fraud filters triggering other filters, and changes in taxpayer filing behaviors due to new tax laws. The officials said they are working to reduce the false detection rate. While it is reasonable to expect fraud filters will catch some legitimate returns, IRS has not conducted a risk assessment—or developed a fraud risk tolerance—consistent with leading practices. Determining a fraud risk tolerance would help officials determine how best to balance the risks of missing fraudulent returns with the risks of flagging legitimate returns. Doing so may also help IRS prioritize any needed improvements to existing filters.

According to the *Fraud Risk Framework*, a fraud risk assessment is the basis for developing an antifraud strategy. Among other things, an antifraud strategy considers the benefits and costs of control activities to address risks, such as the inherent business IDT risks described above, and other risks facing the program. As of July 2019, IRS's Wage and Investment division had identified the overall threat of business IDT as one of 12 risks it is currently facing.

However, IRS's risk documentation does not include important components of a fraud risk assessment consistent with GAO's *Fraud Risk Framework*. Specifically, the documentation does not include information on the likelihood or impact of each risk, IRS's risk tolerance, or clear

³²National Taxpayer Advocate, *Annual Report to Congress 2018* (Washington, D.C.: February 2019). Each year, the National Taxpayer Advocate uses this report to identify at least 20 of the nation's most serious tax problems.

³³This rate represents what IRS officials refer to as the "operational" false detection rate, which does not include cases that IRS reviewed manually.

plans or responsibilities for mitigating risks. A business IDT fraud risk assessment with these key items would position IRS to develop a fraud risk profile and an antifraud strategy for business IDT going forward.

In addition, officials from IRS's Office of the Chief Risk Officer stated that consistent with the Fraud Reduction and Data Analytics Act of 2015 (FRDAA), the agency compiles an annual enterprise-wide fraud risk report based on program-level risks that IRS business units identify and monitor. The Office of the Chief Risk Officer's October 2019 report acknowledges business IDT as one of 11 enterprise fraud risks for 2019–2020.³⁴ A fraud risk assessment and a fraud risk profile on business IDT consistent with leading practices would also help support IRS's broader efforts to report and monitor enterprise-wide fraud risks.

IRS officials stated that they have not performed a formal fraud risk assessment or developed a fraud risk profile for business IDT because they have directed their resources toward identifying and addressing fraud that is occurring right now and improving fraud detection efforts. When asked whether they had plans to further identify and assess inherent fraud risks for business IDT—the first step of the fraud risk assessment process—IRS officials said they thought that the costs of identifying and assessing inherent risks of business IDT would likely outweigh the benefits given the relatively low volume of confirmed business IDT cases, compared with individual IDT refund fraud.

Without assessing inherent risks, determining the likelihood, impact, and IRS's tolerance for each risk, and examining the suitability of existing fraud controls, IRS lacks reasonable assurance that it is aware of the most significant fraud risks facing business IDT. Such an analysis would also help IRS determine whether additional fraud controls are needed and whether to make adjustments to existing controls.

Further, without this critical information, IRS will be unable to develop a fraud risk profile consistent with leading practices. A fraud risk profile for business IDT may help IRS make better informed decisions about allocating resources to combat business IDT and minimize financial losses. Consistent with our *Fraud Risk Framework*, a fraud risk profile that considers the likelihood and impact of fraud risks, IRS's tolerance for

³⁴We evaluated documents IRS developed related to business IDT risks, but did not evaluate IRS's enterprise-wide risk report or its process for compiling enterprise risks.

Collecting Additional Data
Could Help IRS Estimate the
Size and Scope of Business
IDT

risk, and the suitability of existing fraud detection activities is critical for developing an antifraud strategy and ensuring that IRS has an effective approach to addressing risks to business IDT.

The *Fraud Risk Framework* states that managers may conduct quantitative or qualitative assessments, or both, to help determine the likelihood and impact of inherent fraud risks on the program's objectives and help estimate fraud losses and frequency. Further, federal internal control standards call for program managers to use quality information to achieve their objectives, address relevant risks, and communicate that information as necessary to internal and external stakeholders.³⁵

As of September 2019, IRS was collecting fraud filter data for some, but not all, business-related forms that may be susceptible to business IDT. Our analysis of IRS's data shows that for 2018, business IDT fraud filters covered about 88 percent of business tax forms claiming a refund (14.0 million out of 15.9 million returns) and nearly all employment tax forms claiming a refund (30.7 million out of 31.0 million returns). IRS officials stated that since 2016, they have incrementally implemented business IDT fraud filters for the most commonly filed forms.

We recognize that IRS has made progress in implementing filters for commonly filed forms and that the deceptive nature of fraud makes developing accurate fraud estimates challenging. However, our analysis shows that IRS has not developed business IDT fraud filters for at least 25 additional business-related tax forms. In 2018, these forms represented about \$10.4 billion in refunds. As a result, IRS is not able to analyze data from these forms for emerging fraud patterns or schemes.

Further, while current business IDT fraud filters cover the most commonly filed forms, IRS has not assessed which remaining forms or fraud scenarios pose the greatest risk to IRS and taxpayers. IRS also has not determined a risk tolerance for existing fraud filters, and whether the benefits of expanding existing filters outweigh the risks of flagging legitimate returns. Given the complexity of business tax forms and the evolving nature of fraud schemes, IRS's existing fraud filters may not be sufficient to detect different business IDT scenarios. For example, IRS

³⁵GAO-14-704G. Quality information is appropriate, current, complete, accurate, accessible, and provided on a timely basis.

has implemented two fraud filters related to business tax credits, but they are each limited to a specific scenario.

TIGTA has previously reported that tax credit forms have been found to be attractive to fraudsters. For example, in 2015, TIGTA reported that fraudsters have targeted individual tax credits when filing a fraudulent tax return to increase their refund.³⁶ In September 2019, TIGTA reported that IRS lacked systematic controls to identify or prevent fraudulent use of an electric motor vehicle tax credit which is available to individuals and businesses.³⁷

Without additional data on business IDT, IRS cannot estimate the full size and scope of this problem. As we have previously reported, IRS's annual *Identity Theft Taxonomy (Taxonomy)* is a valuable tool to inventory, characterize, and analyze available individual IDT refund fraud data and to assess the performance of IRS's individual IDT refund fraud defenses.³⁸ Following each filing season, IRS estimates the volume of returns and associated dollar amounts on attempted and prevented individual IDT refund fraud, and on refunds it paid to fraudsters.³⁹

While we recognize there may be differences in how IRS estimates the extent of individual versus business IDT, the *Taxonomy* is a useful framework to understand the data IRS needs to estimate the size and scope of business IDT. For example, the *Taxonomy* estimates the number of identified individual IDT refund fraud cases where IRS prevented or recovered the fraudulent refunds (e.g., returns caught by

³⁶Treasury Inspector General for Tax Administration, *Processes Are Being Established to Detect Business Identity Theft; However, Additional Actions Can Help Improve Detection*, 2015-40-082 (Washington, D.C.: Sept. 9, 2015).

³⁷TIGTA identified about \$83 million in erroneous tax credit claims. See Treasury Inspector General for Tax Administration, *Millions of Dollars in Potentially Erroneous Qualified Plug-In Electric Drive Motor Vehicle Credits Continue to Be Claimed Using Ineligible Vehicles*, 2019-30-072 (Washington, D.C.: Sept. 30, 2019).

³⁸Among other things, this effort involves identifying characteristics of fraudulent returns, matching and analyzing information returns and tax returns based on these characteristics, and researching other data sources. See [GAO-14-633](#).

³⁹In its most recent *Taxonomy*, IRS estimates that at least \$11.9 billion in individual IDT refund fraud was attempted in calendar year 2017 and that it prevented the theft of at least \$11.8 billion of that amount. IRS also estimated that it paid between \$110 million and \$600 million to fraudsters. As we have previously reported, because of the difficulties in estimating the amount of undetectable fraud, the actual amounts could differ from IRS's estimates. See [GAO-16-508](#).

fraud filters or suspicious refunds returned by banks). In December 2018, IRS developed a draft plan for an initial business IDT taxonomy based on two business tax forms on which IRS has collected data since 2016. IRS officials stated that they intend to begin preliminary work on this effort in December 2019. However, these efforts will be limited until IRS collects additional data.

IRS officials stated that they are committed to better understanding business IDT and expanding their fraud detection and data collection efforts. However, officials said that doing so depends on the availability of resources to develop and test new fraud filters prior to each filing season. IRS may address these constraints by, for example, determining which forms or fraud scenarios pose the greatest risk for business IDT based on a fraud risk assessment and profile. This would include determining a risk tolerance for business IDT on these forms and prioritizing new filters or filter enhancements based on its risk assessment.

Having additional data to better estimate the size and scope of business IDT is critical in helping IRS understand how fraudsters are evading IRS defenses. Additionally, such data will help IRS identify unknown business IDT fraud risks, allocate limited resources, assess the suitability of its existing fraud control activities, and develop tools such as a business IDT taxonomy. Further information on the size and scope of business IDT could better position IRS to assess the risk of business IDT on tax administration and inform the Congress and the public about the risk.

IRS Has Procedures for Resolving Business IDT Cases, but Has Not Established Customer Service-Oriented Performance Goals

IRS has established procedures for resolving business IDT cases in its Internal Revenue Manual (IRM) and officials described general guidelines for resolving both pre-refund and post-refund business IDT cases. However, IRS does not resolve all cases within these guidelines due to various challenges IRS could potentially address, such as correspondence-based authentication; and challenges which are more difficult to address, such as the overall complexity of business IDT cases. In addition, we found that a lack of customer service-oriented performance goals for resolving cases may also contribute to delays.

Key IRS documents highlight both a commitment to combating IDT refund fraud and improving customer service for taxpayers by, for example, reducing case resolution time frames through new technologies, among

other things.⁴⁰ In addition, Office of Management and Budget guidance highlights that federal program and project managers have an obligation to ensure that their programs deliver efficient and effective services to the public.⁴¹ This includes assessing how well a program is working to achieve intended results, and delivering customer service to align with the program's goals.⁴²

Our review of IRS documentation found that business units have developed procedures to manage and resolve business IDT cases identified during different stages of the tax return process.⁴³ For example, during the pre-refund stage, RICS notifies business taxpayers via mail if their return shows signs of potential IDT refund fraud and has been held for review. Similarly, when a taxpayer notifies IRS about potential IDT refund fraud during the post-refund stage, Accounts Management (AM) may require the taxpayer to submit a form describing how and when the fraud occurred. IRS business units have also established procedures for conducting in-depth research on taxpayer accounts to determine if a case is business IDT or another type of fraud. However, RICS and AM have had some difficulty in resolving cases within their respective guidelines, as described below.

Pre-refund cases. In regards to pre-refund business IDT, cases are generally to be resolved within 90 days, according to IRS's IRM and agency officials.⁴⁴ RICS officials stated that they aim to meet this guideline because it provides enough time to reach the correct taxpayer via mail and for the taxpayer to respond. However, RICS has been challenged in resolving cases within 90 days. Our analysis of pre-refund business IDT cases opened from mid-January 2017 through December

⁴⁰See Internal Revenue Service, *IRS Integrated Modernization Business Plan* (Washington, D.C.: April 2019); Department of the Treasury, *Agency Priority Goal Action Plan for Fraud Prevention, Fiscal Year 2019* (Washington, D.C.: June 2019); and Internal Revenue Service, *IRS Strategic Plan, Fiscal Years 2018-2022* (Washington, D.C.: May 23, 2018).

⁴¹Office of Management and Budget, *Preparation, Submission and Execution of the Budget*, Circular No. A-11, pt. 6, § 270 (June 2019). This guidance implements provisions of the Program Management Improvement Accountability Act. Pub. L. No. 114-264, 130 Stat. 1371 (2016).

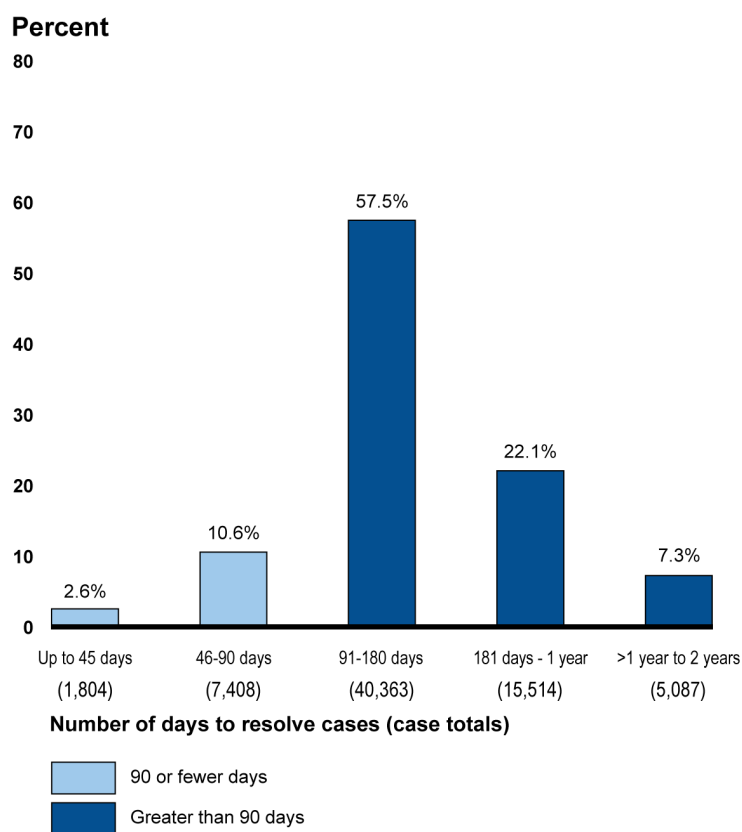
⁴²Office of Management and Budget, Circular No. A-11, pt. 6, §§ 270.8, 270.9 (2019).

⁴³Internal Revenue Manual (IRM) Part 25, Chapters 23 and 25.

⁴⁴IRM Part 25, Chapter 25, Section 1.

2018 shows that RICS did not meet this guideline for about 87 percent of cases, including open cases.⁴⁵ RICS also took between 6 months to 2 years to resolve about 29 percent of cases (see fig. 4).

Figure 4: About 87 Percent of IRS Pre-Refund Business Identity Theft (IDT) Cases Were Not Resolved within 90 Days, Cases Opened from Mid-January 2017 through December 2018



Source: GAO analysis of Internal Revenue Service (IRS) data. | GAO-20-174

Notes: N=70,176 business IDT cases from IRS's Business Master File Identity Check system as of August 2019. Data includes 4,649 cases that IRS had not resolved as of August 2019. Data may not add up to 100 percent due to rounding.

"Number of days to resolve cases" includes days when IRS is waiting for a response from the taxpayer.

⁴⁵We analyzed 70,176 business IDT cases in RICS's inventory as of August 2019. This included 4,649 cases that were still open when we obtained the data from IRS. For these open cases, we manually added the date we received the data as the date the case was closed. This was an indicator of the minimum amount of time RICS could have taken to close these cases.

Further, our analysis found that this delay was consistent across case outcomes. On average, RICS took 136 days to resolve cases of confirmed business IDT (7,248 cases) and 171 days to resolve cases determined not to be business IDT (58,279 cases). As of August 2019, IRS had not resolved 4,649 cases which had been open for an average of 383 days.

RICS officials identified several reasons for the delay in resolving pre-refund cases, including ones rooted in business IDT policies and procedures. Specifically, officials stated that communicating with the taxpayer via correspondence is the primary driver of delays in resolving cases. RICS officials stated that mail-based authentication generally takes more time because letters can get lost, thrown away, or not reach the right person. RICS officials stated that in March 2018, they began making two attempts to correspond with a business with a potentially suspicious return before closing a case, rather than one attempt. RICS made this change because taxpayers were taking longer than 45 days to respond to the letter, often after RICS had closed the case as a nonresponse.

Officials stated that while they are aware of IRS's other methods of authenticating taxpayers for individual IDT refund fraud, such as by phone or in person, they have not explored similar options for the business IDT program. As we reported in June 2018, IRS uses a risk-based approach to determine the ways in which a taxpayer can authenticate his or her identity and what data are required during the authentication process.⁴⁶ High risk interactions include those when a taxpayer accesses prior year tax information and other PII, while lower risk interactions include a taxpayer paying a bill online. According to IRS officials, as the risk level of taxpayer interactions increases, the authentication process becomes more rigorous. This approach minimizes risk to both the taxpayer and IRS.

In addition, officials identified other challenges that contribute to delays, including incorrect information on the business taxpayer's account, nonresponses to authentication requests, and the complexity of business IDT cases, which may be more difficult to address. RICS officials noted that taxpayers do not always update the business's responsible party with IRS when they sell or transfer a business to someone else. This can

⁴⁶[GAO-18-418](#).

make it more difficult for IRS to contact the taxpayer when their return has been selected for review. RICS officials stated that IRS reminds business taxpayers to check and update their information each year to avoid unnecessary delays in processing tax returns; however, IRS does not require taxpayers to make updates.

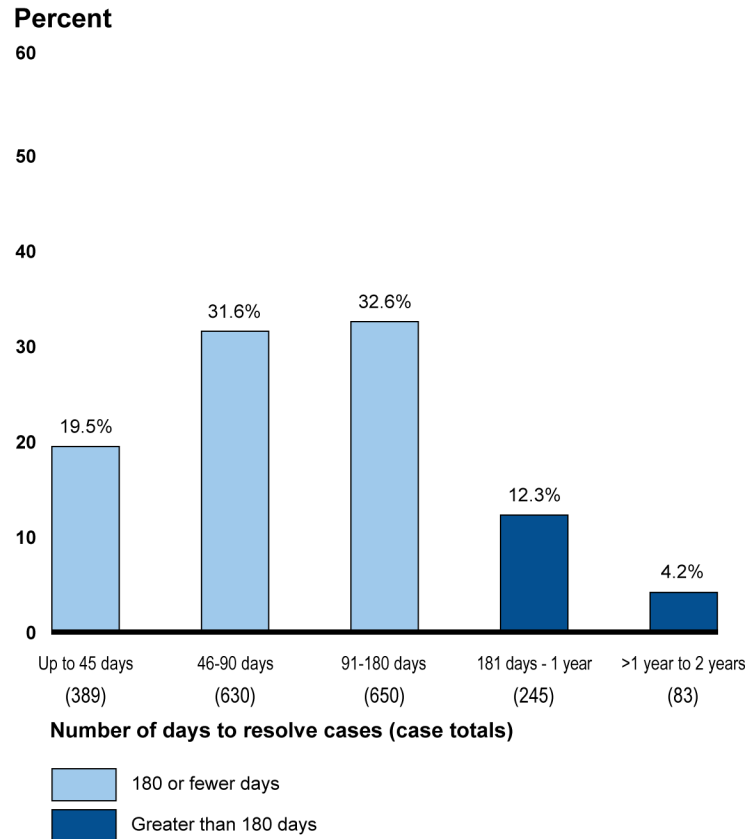
IRS officials also stated that a business's failure to respond to mail-based authentication requests contributes to case resolution delays. Finally, RICS officials noted that the inherent complexity of the business IDT environment may require RICS staff to research cases across multiple IRS business units or refer cases outside of RICS, which can contribute to delays.

Post-refund cases. Our review of AM procedures and discussions with officials indicate that post-refund business IDT cases are generally to be resolved within 6 months.⁴⁷ AM officials stated they established this guideline for individual IDT refund fraud cases and extended it to business IDT cases when the program started in 2016. We analyzed post-refund cases that AM opened from July 2016 (when IRS began collecting data) through December 2018.⁴⁸ We found that AM resolved about 84 percent of post-refund cases within 6 months. However, about 17 percent of these cases—including open cases—took more than 6 months to resolve (see fig. 5).

⁴⁷IRM Part 25, Chapter 23, Section 11.

⁴⁸We analyzed 1,997 business IDT cases in AM's inventory as of June 2019. This included 170 cases that were still open when we obtained the data from IRS. For these open cases, we manually added the date we received the data as the date the case was closed. This was an indicator of the minimum amount of time AM could have taken to close these cases.

Figure 5: About 17 Percent of IRS Post-Refund Business Identity Theft (IDT) Cases Were Not Resolved within 6 Months, Cases Opened July 2016 through December 2018



Source: GAO analysis of Internal Revenue Service (IRS) data. | GAO-20-174

Note: N=1,997 business IDT cases from IRS's Correspondence Imaging System as of June 2019. Data includes 170 cases that IRS had not resolved as of June 2019. Data may not add up to 100 percent due to rounding.

Similar to RICS officials, AM officials cited several reasons for case resolution delays, including the complexity of the business tax environment and the need to research associated businesses, employment, and individual tax returns. AM officials also noted challenges inherent to the case research process, including that staff often pursue multiple lines of inquiry to determine a case outcome. This may involve referring cases to other business units if, for example, AM staff do not have access to a specific IRS system to complete their research.

Finally, AM officials stated that AM staff do not always recognize business IDT cases and may initially classify them as an individual IDT case, which results in delays. To help address this issue, AM officials stated that management periodically reviews business IDT operations, and provides refresher training in areas where staff did not follow procedures consistently.

While RICS and AM officials have stated that they have general guidelines for resolving business IDT cases, they have not established customer service-oriented performance goals. We have previously found that a fundamental element in an organization's efforts to manage for results is its ability to set meaningful goals for performance, including customer service standards, and to measure progress toward those goals.⁴⁹ Standards that include customer service-oriented performance targets or goals allow agencies to define, among other things, the level, quality, and timeliness of the service they provide to their customers.

In the context of IRS's business IDT efforts, a customer service-oriented goal could be, for example, to resolve a certain percentage of cases within a specific timeframe. This is particularly important for IRS because one of its strategic goals is to empower customers to meet their tax obligations by providing exceptional customer service.

Identifying and implementing methods to address challenges that IRS can control—such as reliance on correspondence-based authentication—could help IRS improve its timeliness in resolving business IDT cases and address its overall strategic objective to reduce case resolution time frames. It is also consistent with OMB guidance to deliver efficient and effective services to the public. Further, establishing customer service-oriented performance goals could help IRS measure progress, identify opportunities for improvement, and communicate reasonable time frames for resolving cases to taxpayers.

Case resolution performance goals may also help reduce costs to the Treasury. Specifically, IRS has a legal obligation to pay interest on

⁴⁹For examples, see GAO, *Managing for Results: Further Progress Made in Implementing the GPRA Modernization Act, but Additional Actions Needed to Address Pressing Governance Challenges*, [GAO-17-775](#) (Washington, D.C.: Sept. 29, 2017); *Managing for Results: Selected Agencies Need to Take Additional Efforts to Improve Customer Service*, [GAO-15-84](#) (Washington, D.C.: Oct. 24, 2014); *Managing for Results: Executive Branch Should More Fully Implement the GPRA Modernization Act to Address Pressing Governance Challenges*, [GAO-13-518](#) (Washington, D.C.: June 26, 2013).

refunds issued after 45 days from the due date of the tax return.⁵⁰ This requirement includes incoming tax returns that IRS holds for review for potential business IDT but then later releases for processing. Specific and relevant performance goals for both pre-refund and post-refund cases may help IRS balance its efforts to protect revenue against the burden on legitimate taxpayers and additional costs to the Treasury.

Conclusions

IRS has recognized business IDT as a growing threat to both taxpayers and tax administration. The complexity of the business tax environment—including different business types and taxes that businesses must pay—makes detecting, researching, and resolving potential business IDT cases more challenging for IRS compared with individual IDT cases. IRS has taken important steps to prevent business IDT, including using fraud filters to screen incoming business returns on selected forms and collaborating with state and industry partners to identify and respond to potentially suspicious activity.

IRS leadership has demonstrated an overall commitment to identifying and combating IDT refund fraud. However, IRS has not designated a lead entity to design and oversee business IDT fraud risk management activities consistent with leading practices. A lead entity could also help IRS ensure its business IDT activities are better coordinated to combat the evolving threat of business IDT.

Further, while IRS has taken some steps to understand business IDT fraud risks, it has not developed a fraud risk profile based on an assessment of inherent risks, the likelihood and impact of risks, IRS's risk tolerance, and an evaluation of existing fraud controls. Assessing inherent fraud risks, such as those that we highlighted—correspondence-based authentication, vulnerability of EINs, and a high false detection rate for IDT fraud filters—would help IRS to establish a fraud risk tolerance and form the basis for an antifraud strategy. IRS has made progress in detecting and preventing business IDT by implementing fraud filters and collecting data on six business-related tax forms.

However, without a risk profile, IRS does not have assurance that its existing filters mitigate inherent risks. For example, risks may also be associated with at least 25 other tax forms, and IRS has not determined

⁵⁰26 U.S.C. § 6611.

which forms or fraud scenarios pose the greatest risk to IRS and taxpayers based on an analysis of risk. Collecting additional data by implementing new fraud filters would better position IRS to estimate the full size and scope of business IDT.

IRS's planning documents articulate a commitment to reducing case resolution time frames and improving customer service, but RICS and AM have been delayed in resolving business IDT cases due to various challenges. Identifying and implementing ways to address the challenges IRS can control, such as its methods for taxpayer authentication, and establishing customer service-oriented case resolution performance goals could help IRS better serve taxpayers and minimize additional costs to the Treasury.

Recommendations for Executive Action

We are making the following six recommendations to IRS:

The Commissioner of Internal Revenue should designate a dedicated entity to provide oversight of agency-wide efforts to detect, prevent, and resolve business IDT, consistent with leading practices. This may involve designating one business unit as a lead entity or leveraging cooperative relationships between business units to establish a business IDT leadership team. This entity should have defined responsibilities and authority for managing fraud risk. (Recommendation 1)

The Commissioner of Internal Revenue should develop a fraud risk profile for business IDT that aligns with leading practices. This should include (1) identifying inherent fraud risks of business IDT, (2) assessing the likelihood and impact of inherent fraud risks, (3) determining fraud risk tolerance, and (4) examining the suitability of existing fraud controls. (Recommendation 2)

The Commissioner of Internal Revenue should develop, document, and implement a strategy for addressing fraud risks that will be identified in its fraud risk profile. (Recommendation 3)

The Commissioner of Internal Revenue should ensure that IRS collects additional data on business IDT by identifying and implementing new fraud filters consistent with its fraud risk profile. This should include prioritizing IDT filters for tax forms determined to be most at risk based on an analysis of risk tolerances. (Recommendation 4)

The Commissioner of Internal Revenue should identify and implement methods to address delays in resolving business IDT cases due to correspondence-based authentication. This could involve using different methods for taxpayer authentication based on the risk level of the return. (Recommendation 5)

The Commissioner of Internal Revenue should establish customer service-oriented performance goals for resolving business IDT cases. (Recommendation 6)

Agency Comments and Our Evaluation

We provided a draft of this report to IRS for review and comment. In written comments, which are summarized below and reproduced in appendix II, IRS's Deputy Commissioner for Services and Enforcement agreed with five of our six recommendations and neither agreed nor disagreed with one of our recommendations.

IRS agreed with our four recommendations to better identify, assess, and manage business IDT fraud risks consistent with leading practices in our *Fraud Risk Framework*. IRS agreed to designate a dedicated entity to provide oversight of agency-wide business IDT efforts and stated that it will determine the appropriate oversight structure and scope of authority. IRS also agreed with our recommendations to, consistent with leading practices, develop a business IDT fraud risk profile; develop, document, and implement a strategy for addressing fraud risks; and implement and prioritize new fraud filters consistent with its fraud risk profile. IRS did not provide details on the actions it plans to take to address these recommendations.

In its written comments, IRS stated that formally implementing leading practices in the *Fraud Risk Framework* may be helpful, but noted that it has consistently completed business IDT fraud risk assessments and developed risk profiles. However, during our review, IRS did not provide evidence that it had taken such actions. Figure 3 in our report outlines leading practices for performing a fraud risk assessment and developing a risk profile.

For example, regarding the leading practice to identify and assess inherent fraud risks, IRS stated that it has found that the risks associated with in-person or telephone authentication are higher for business IDT than correspondence-based authentication. However, we could not verify this assertion, as IRS did not provide evidence during our audit that it had assessed the risks of different authentication options for business

taxpayers.⁵¹ Further, IRS stated that our report does not acknowledge that multiple individuals may be authorized to act on behalf of a business, including authenticating a potentially suspicious tax return. We have added this information to our report.

IRS also stated that our report implies that it would be acceptable for a percentage of potentially fraudulent returns to be filed, unchecked, solely to reduce false detections or business costs. However, as we indicate in our report, fraud risk tolerance does not mean IRS management tolerates fraud, or that it needs to eliminate controls to detect and prevent fraud. Rather, it means that IRS management accepts a certain amount of risk, based on its assessment of the likelihood and impact of the fraud. Determining a fraud risk tolerance would help IRS management establish appropriate and cost-effective controls that are commensurate with the fraud risk. Relatedly, we agree with IRS's statement that IDT victims suffer significant financial, social, and emotional hardships. We have updated the report's introduction to acknowledge these hardships.

In addition, IRS stated that its work on business IDT filters is more robust than stated in our report. Our report recognizes various IRS efforts to improve business IDT fraud detection and prevention, including efforts to refine its fraud filters. However, having fraud filters does not preclude IRS from identifying and assessing other potential fraud risks. Further, IRS cannot accurately determine the suitability of its business IDT filters—or other controls—without first identifying inherent fraud risks, assessing the likelihood and impact of those risks, and determining a fraud risk tolerance. Additionally, IRS did not provide evidence that it has examined the suitability of other antifraud controls, including controls to prevent fraudsters from obtaining new EINs using stolen information.

IRS neither agreed nor disagreed with our recommendation to establish customer service-oriented performance goals for resolving business IDT cases. However, IRS stated that it will review its customer service-oriented performance goals and modify them, as warranted, to address

⁵¹In June 2018, we reported that IRS had not established internal controls for its telephone, in-person, and correspondence methods of authenticating taxpayers. We recommended that IRS establish a policy for conducting risk assessments for these methods and develop a plan for performing risk assessments. As of November 2019, IRS had developed a draft policy for conducting risk assessments. However, IRS had not yet developed a plan for performing these assessments. IRS officials stated that they intend to address these recommendations by May 2020. See [GAO-18-418](#).

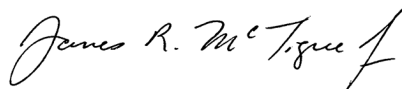
the resolution of business IDT cases. Doing so would meet the intent of our recommendation.

In its written comments, IRS stated that our report does not fully address obstacles that prevent timely case resolution. We have revised our discussion of pre-refund cases to more clearly identify nonresponses from taxpayers as a cause for delays. IRS also said our methodology for determining the time to close business IDT cases does not adequately consider the impact of nonresponses on the agency's ability to close cases in a timely manner. We have added a note to figure 4 to acknowledge the challenge of nonresponses. However, IRS did not provide evidence during the audit that it collects data on how long a case is suspended while it waits for the taxpayer to respond—information that would provide insight into the challenges associated with resolving business IDT cases in a timely manner.

As agreed with your offices, we plan no further distribution of this report until 30 days from the report date. At that time, we will send copies to the Chairmen and Ranking Members of other Senate and House committees and subcommittees that have appropriation, authorization, and oversight responsibilities for IRS. We will also send copies of the report to the Commissioner of Internal Revenue and other interested parties. In addition, this report will be available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff has any questions about this report, please contact me at (202) 512-9110 or mctiguej@gao.gov. Contact points for our offices of Congressional Relations and Public Affairs are on the last page of this report. GAO staff members who made major contributions to this report are listed in appendix III.

Sincerely yours,



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

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) describe the Internal Revenue Service's (IRS) efforts to detect business identity theft refund fraud (business IDT), (2) evaluate the extent to which IRS's efforts to prevent business IDT are consistent with selected fraud risk management leading practices, and (3) assess IRS's efforts to resolve business IDT cases. In this report, business IDT refers to the fraudulent use of both business and employment tax forms. Both of these types of forms require an Employer Identification Number (EIN) when filing with IRS, and a fraudster can file these forms to obtain a refund.¹

To address all of our objectives, we reviewed our prior reports on individual identity theft refund fraud and the Treasury Inspector General for Tax Administration's (TIGTA) prior reports on business IDT.² We also interviewed IRS officials from business units responsible for detecting, preventing, and resolving business IDT cases, specifically from Return Integrity and Compliance Services (RICS), Accounts Management (AM), and Criminal Investigation (CI). In December 2018, we visited IRS's campus in Ogden, Utah, to interview officials responsible for IRS's business IDT efforts and to observe how RICS and AM staff process and research business IDT cases using IRS information technology systems and tools.

To describe IRS's current processes to detect business IDT refund fraud, we reviewed documentation describing the business IDT fraud filters IRS implemented from 2017 through 2019, including the logic for each filter and the forms to which they apply. In addition, we analyzed data from IRS's Dependent Database (DDb) on business IDT fraud filter results for applicable incoming business and employment tax returns IRS received from mid-January 2017 through mid-August 2019.³ This was the most recent, complete, and available set of data at the time of our review. This

¹In contrast, employment fraud occurs when an identity thief uses a taxpayer's name and Social Security number to obtain a job. GAO has ongoing work on employment-related identity fraud and expects to issue a report on the results in early 2020.

²For example, our review included GAO, *Identity Theft: IRS Needs to Strengthen Taxpayer Authentication Efforts*, [GAO-18-418](#) (Washington, D.C.: June 22, 2018); *Identity Theft and Tax Fraud: IRS Needs to Update Its Risk Assessment for the Taxpayer Protection Program*, [GAO-16-508](#) (Washington, D.C.: May 24, 2016); and Treasury Inspector General for Tax Administration, *Processes Are Being Established to Detect Business Identity Theft; However, Additional Actions Can Help Improve Detection* 2015-40-082 (Washington, D.C.: Sept. 9, 2015).

³January 13, 2017, was the earliest available data for 2017.

analysis showed the volume of returns selected by IRS's business IDT fraud filters by form, tax processing year, and associated refund amount.

We also analyzed data from IRS's Business Master File Identity Check (BMFIC) system—RICS's case management system for business IDT returns flagged by DDb—for cases opened from mid-January 2017 through mid-August 2019.⁴ These were the most complete set of data available at the time of our review. Our analysis of BMFIC data showed the number of returns that RICS researched as potential business IDT, the outcome of the case, and associated refund amounts. For the purpose of analysis and reporting, we grouped business IDT case outcomes into three categories: confirmed business IDT, not business IDT, and open/unresolved.⁵

We assessed the reliability of data from these systems by: (1) testing key data elements, including checks for missing, out-of-range, or logically inaccurate data; (2) reviewing documents for information about the data and IRS's systems; and (3) interviewing officials knowledgeable about the data to discuss any limitations. We determined that these data were sufficiently reliable to describe the volume of incoming returns stopped by business IDT fraud filters, associated refunds, and the outcome of business IDT cases.

To understand IRS's efforts to collaborate with external partners to detect and prevent business IDT, we interviewed IRS and state officials from the Security Summit's Business IDT sub-workgroup and reviewed IRS's 2018 report which analyzed business-related data elements from incoming tax returns.⁶ We also interviewed IRS officials about a pilot program with the Alabama Department of Labor to help detect and deactivate potentially

⁴Not all returns selected by DDb become business IDT cases in BMFIC. IRS officials stated that some returns may be erroneously selected by fraud filters due to unforeseen circumstances, such as unanticipated effects from tax law changes. Officials stated that these returns may be subsequently released for processing.

⁵"Confirmed business IDT" represents cases categorized in BMFIC as confirmed business IDT, and those where the taxpayer did not respond to IRS's letter to authenticate their identity. "Not business IDT" represents cases categorized in BMFIC as not IDT; frivolous returns that contain unsupported tax arguments; or cases that are manually reviewed by RICS due to, for example, a high refund amount. "Open/unresolved" represents cases with no recorded outcome in BMFIC.

⁶Each Security Summit full workgroup is led by three "co-leads"—one each from IRS, state departments of revenue or state associations, and industry partners.

suspicious EINs established in that state. For context, we obtained information from January to December 2018 from IRS on the performance of this pilot, including the number of EINs identified as fraudulent.

To evaluate the extent to which IRS's efforts to prevent business IDT are consistent with selected fraud risk management leading practices, we reviewed the Fraud Reduction and Data Analytics Act (FRDAA) of 2015 and leading practices outlined in *A Framework for Managing Fraud Risks in Federal Programs (Fraud Risk Framework)*.⁷ We generally focused our review on the first two components of the *Fraud Risk Framework*: (1) commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management, and (2) plan regular fraud risk assessments and assess risks to determine a fraud risk profile.⁸ We reviewed agency documents and information obtained from interviews, as described below, and compared them against leading practices identified in the *Fraud Risk Framework* related to these two components.

- We reviewed IRS's most recent strategic planning documents related to reducing fraud, IRS organizational charts, and relevant Internal Revenue Manual (IRM) sections on business IDT operations and procedures.⁹ We interviewed officials from RICS, AM, CI, and the Office of Research, Applied Analytics, and Statistics (RAAS) to understand each business unit's respective role in detecting, preventing, and resolving business IDT cases and the extent to which

⁷Pub. L. No. 114-186, § 3, 130 Stat. 546 (2016). The Fraud Reduction and Data Analytics Act of 2015 requires the Office of Management and Budget (OMB) to establish guidelines that incorporate the leading practices of GAO's *Fraud Risk Framework*. The act also requires federal agencies to submit to Congress a progress report each year, for 3 consecutive years, on implementation of the risk management and internal controls established under the OMB guidelines. See GAO, *A Framework for Managing Fraud Risks in Federal Programs*, [GAO-15-593SP](#) (Washington, D.C.: July 28, 2015).

⁸The other components of the *Fraud Risk Framework* are: (3) design and implement a strategy with specific control activities to mitigate assessed risks and collaborate to ensure effective implementation; and (4) evaluate outcomes using a risk-based approach and adapt activities to improve fraud risk management. We did not formally assess IRS's business IDT efforts against these components of the *Fraud Risk Framework* given that IRS has not yet addressed the first two components.

⁹These documents include Internal Revenue Service, *IRS Strategic Plan, Fiscal Years 2018-2022* (Washington, D.C.: May 23, 2018); *IRS Integrated Modernization Business Plan* (Washington, D.C.: April 2019); *IRS Agency Priority Goal Action Plan for Fraud Prevention, Fiscal Year 2019, Quarter 3* (Washington, D.C.: June 2019); and IRM Part 25, Chapters 23 and 25.

business units work together on day-to-day and longer-term efforts. In addition, we reviewed IRS reports on business IDT case workload. We also reviewed meeting notes from IRS's IDT Executive Steering Committee (July and October 2017, and January and October 2018) to understand the extent to which IRS's executive-level groups are, for example, involved in helping guide business IDT efforts or made aware of business IDT challenges.

- We interviewed officials from RICS, AM, CI, and RAAS and reviewed documentation on IRS's efforts to identify and assess business IDT fraud risks. These included reviewing RAAS's analyses on business IDT fraud filter performance, descriptions of potential new fraud filters that IRS may implement in the future, and the Wage and Investment Division's risk register. We also interviewed officials from IRS's Office of the Chief Risk Officer to understand IRS's efforts to compile and report on enterprise-wide fraud risks and agency efforts to develop an antifraud culture.

Further, we reviewed documentation related to three inherent fraud risks to business IDT that we identified in the course of our work: correspondence-based authentication, EIN vulnerabilities, and high false-detection rates for IDT fraud filters.¹⁰ This included reviewing prior GAO, TIGTA, and National Taxpayer Advocate reports and the status of open recommendations, and relevant IRM sections.¹¹ We reviewed the methodologies of these reports and found them reasonable for the purpose of describing the inherent risks related to business IDT.

In addition, we identified a false detection rate for business IDT fraud filters based on BMFIC cases opened from mid-January 2017 through December 2018. To do so, we compared the number of cases IRS determined were not business IDT, relative to the total number of cases.¹² We did not include BMFIC cases from 2019 because at the

¹⁰In this context, the false detection rate is the percentage of legitimate returns selected by the IRS as potentially fraudulent, divided by the total number of returns selected as potentially fraudulent.

¹¹See [GAO-18-418](#); Treasury Inspector General for Tax Administration, *Actions Are Needed to Reduce the Risk of Fraudulent Use of Employer Identification Numbers and to Improve the Effectiveness of the Application Process*, 2018-40-013 (Washington, D.C.: Feb. 7, 2018); and National Taxpayer Advocate, *Annual Report to Congress 2018* (Washington, D.C.: February 2019).

¹²In our report, we present what IRS officials refer to as the "operational" false detection rate. This rate does not include cases that IRS reviewed manually.

time of our analysis, about 27 percent of those cases were unresolved.

- We also assessed the extent to which IRS is positioned to estimate the size and scope of business IDT. To do so, we reviewed documents and information on IRS's efforts to collect quality data on incoming business and employment returns. We compared these efforts to leading practices associated with the first two components of the *Fraud Risk Framework and Standards for Internal Control in the Federal Government* related to using quality information.¹³ Specifically, we determined what proportion of incoming business and employment tax forms filed in 2018 would have been screened by business IDT fraud filters, by tax form type. We also reviewed a preliminary plan and interviewed RAAS and RICS officials on their efforts to develop a business IDT taxonomy.¹⁴

To assess IRS's efforts to resolve business IDT cases, we reviewed IRS procedures for managing, researching, and resolving pre-refund and post-refund business IDT cases.¹⁵ We interviewed officials from RICS and AM to understand the rationale behind their respective current case resolution time frames, and potential reasons for case resolution delays. We compared RICS and AM's efforts to resolve business IDT cases against Office of Management and Budget guidance on program management and providing customer service.¹⁶ To determine RICS's performance in resolving business IDT cases identified during the pre-refund phase, we analyzed 181,032 cases from BMFIC, described above.

¹³GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 10, 2014).

¹⁴We have previously reported on IRS's annual individual *Identity Theft Taxonomy* (for example, 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). IRS's *Taxonomy* effort helps the agency inventory, characterize, and analyze available individual IDT refund fraud data and assess the performance of individual IDT refund fraud defenses. It also helps IRS estimate the volume of returns and associated dollar amounts on attempted and prevented individual IDT refund fraud, and on refunds it paid to fraudsters.

¹⁵Specifically, we reviewed IRM Part 25, Chapter 23 (post-refund business IDT) and Chapter 25 (pre-refund business IDT).

¹⁶Office of Management and Budget, *Preparation, Submission and Execution of the Budget*, Circular No. A-11, pt. 6, § 270 (June 2019). This guidance implements provisions of the Program Management Improvement Accountability Act. Pub. L. No. 114-264, 130 Stat. 1371 (2016).

Specifically, we calculated the duration between when RICS opened the case in BMFIC to when the case was closed. In addition, we determined how many cases in RICS's inventory were open at the time of our analysis in August 2019. For these open cases, we manually added the date we received the data as the date the case was closed. This was an indicator of the minimum amount of time RICS could have taken to close these cases.

For this analysis, we did not include cases opened and closed in 2019 because we wanted to ensure there was sufficient time for RICS to research and close a case. We determined that cases opened by the end of December 2018 gave both RICS and AM (discussed below) enough time to resolve a case. In addition, we identified an anomaly in RICS's 2019 cases. IRS officials stated that a new fraud filter inaccurately flagged incoming returns on one form, and IRS released these returns. Our analysis of RICS's data showed that these returns accounted for about 65 percent of closed cases in 2019, and that they were resolved in an unusually short time frame (fewer than 45 days) thus skewing the overall data. We also did not include 1,679 cases that were opened and closed in zero or fewer days.¹⁷

To determine AM's performance in resolving business IDT cases identified during the post-refund phase, we analyzed 1,997 relevant business IDT cases from IRS's Correspondence Imaging System (CIS) that AM opened from July 2016 through December 2018.¹⁸ As discussed earlier, we did not include cases opened and closed in 2019 to allow AM enough time to research and resolve a case. We calculated the duration between when AM opened the case in CIS to when the case was closed. We also determined how many cases in AM's inventory were open at the time of our analysis. For these open cases, we manually added the date we received the data as the date the case was closed. This was an indicator of the minimum amount of time AM could have taken to close these cases. We assessed the reliability of the CIS data by reviewing relevant documents, testing key data elements, and interviewing knowledgeable IRS officials. We determined that the data from CIS was

¹⁷IRS indicated that these cases were closed prior to the March 2018 implementation of BMFIC, which led to erroneous data in the system. We confirmed that the majority of cases showing zero or fewer days to close were from 2017, consistent with IRS's explanation.

¹⁸IRS began collecting these data in CIS in July 2016.

sufficiently reliable to determine how long it took AM to resolve post-refund business IDT cases during this time period.

We conducted this performance audit from July 2018 to January 2020 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: Comments from the Internal Revenue Service



DEPUTY COMMISSIONER

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

January 10, 2020

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

Dear Mr. McTigue:

I have reviewed the draft report entitled *IDENTITY THEFT: IRS Needs to Better Assess the Risks of Refund Fraud on Business-Related Returns* (GAO-20-174), and appreciate the opportunity to provide comments. I also appreciate the report's acknowledgement of our commitment to identifying and combating identity theft (IDT) refund fraud. The proliferation of refundable tax credits in the Internal Revenue Code, available to both individuals and businesses, are attractive targets to fraudsters who employ criminal means to obtain benefits to which they are not entitled. These unscrupulous individuals persistently attack the tax system, looking for vulnerabilities to exploit. Business IDT is a very complex issue compounded by the number of different types of business entities and the volume of tax obligations associated with them. Similar to the processes used to build and fortify our defenses against individual IDT refund fraud, we are developing proactive, protective measures to combat business IDT refund fraud. From January 2017 through August 2019, we identified 182,700 business returns having indications of potential IDT refund fraud and, after additional review, confirmed 7,900 were IDT refund claims and stopped the associated \$384 million in refunds claimed on them.

In reviewing the draft report, we found some areas of concern. The benchmark used in your evaluation assesses how the IRS applied leading practices, as outlined in the Government Accountability Office's (GAO's) *A Framework for Managing Fraud Risks in Federal Programs (Fraud Risk Framework)*¹. The report states that IRS has not conducted a fraud risk assessment or developed a risk profile for business IDT consistent with the *Fraud Risk Framework's* leading practices. While we have not followed the structure outlined in the GAO's framework, we have consistently completed fraud risk assessments and developed risk profiles through every step of administering our response to business IDT. We acknowledge that a formal implementation of the leading practices found in the *Fraud Risk Framework* may be helpful.

¹ GAO-15-593SP (Washington D.C.: July 28, 2015).

The assessments used by the IRS have driven the development and refinement of the filters used, how we communicate with the taxpayer entity and responsible individuals, and how we determine which returns are at high risk of potential IDT. We leverage lessons learned from the individual IDT assessments, using them to more effectively address business IDT.

We use a correspondence-based authentication process in lieu of other options, such as in-person or by telephone. The report states that authentication by correspondence may have a lower assurance rate that the respondent is the actual business owner and the return in question is legitimate. The report does not, however, acknowledge that for corporations, partnerships, estates and trusts, there are often multiple individuals authorized to act on behalf of the entity. When we issue letters to the entities identified as potential IDT victims, we issue the letter to both the entity and the individual taxpayer listed as the responsible party. When the written responses are received from both parties, we compare them. Comparison of the responses gives us the ability to identify fabricated business entities that were established using stolen individual information. Using in-person or telephone authentication likely would not yield the same results and there would be a greater risk of the return being processed and the associated refund being paid. We have found that the risk of in-person or telephone authentication is higher for business IDT than correspondence-based authentication. Using correspondence-based authentication gives the IRS more assurance that the entity and return are legitimate. However, we recognize there are opportunities to improve and we will continue exploring them to improve the authentication processes.

Additionally, the report states that we have not developed a fraud risk tolerance to determine how best to balance the risks of missing fraudulent returns with the risk of flagging legitimate returns. However, the report does not recognize that all IDT victims, whether businesses or individuals, suffer significant financial, social, and emotional hardships when an IDT fraudulent filing, based on acceptable risk, is allowed. A risk assessment was completed for the individual IDT victim protection processes and its results are also applicable to business IDT processes. We are concerned with the implication that it would be acceptable for a percentage of IDT returns to be filed, unchecked, solely to reduce false detections or business costs. We continually evaluate changes in the tax system and improve our refund fraud detection methods, including refining our filters. We regularly improve the filters, using a variety of methodologies, algorithms, data sets, and techniques to stay ahead of fraudsters. We evaluate and monitor the performance of each filter on a routine basis and adjust those that are not performing as expected. We apply lessons learned from confirmed cases and consider emerging trends. Each year, in consideration of historical patterns, we rebuild and refresh our filters and models to better detect emerging schemes. In our Security Summit and Information Sharing and Analysis Center, we partner with financial institutions, and state and local governments, to share information on current IDT

3

trends, data breaches, and methods for improved IDT detection and protection for both individuals and businesses.

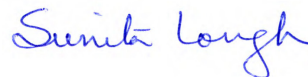
The IRS views its detection rates within the context of the fraud landscape. Fraud that the IRS does not detect has a significant burden on legitimate taxpayers and results in lost government revenue. Our work in individual IDT, using this model, validates that the IRS's fraud detection strategy has resulted in fewer taxpayers falling victim to identity theft. By detecting fraud at the time of tax return submission, we protect the accounts of legitimate taxpayers. We recognize the scale of the business-related and individual IDT are different; however, both have significant monetary impacts to the government.

Our work with the business IDT filters is more robust than stated in the report. During this audit we had 38 discrete projects and, historically, complete between 15 and 17 annually. Filter development leverages the data available in the Return Review Program (RRP), and we continue to expand the number of forms covered as we combat business-related IDT. In addition to using the fraud detection capabilities of the RRP, we also use an offline process, independent of the RRP, to provide supplemental continuous monitoring.

We recognize there is an opportunity for improvement in the establishment of customer service-oriented performance goals; however, it should be noted that we strive to resolve cases within a 90-day timeframe. The report does not fully address obstacles that impede timely case resolution, such as instances where taxpayers (business entities or responsible individuals) do not respond to authentication inquiries. Failure to respond prevents suspended returns from being resolved timely. We disagree with the methodology used in the report's assessment of timeliness, as it does not adequately consider the impact non-responses have on case closures. This presents an incomplete assessment and can be misleading to third-party readers.

Responses to your specific recommendations are enclosed. If you have any questions, please contact Michael Beebe, Director, Return Integrity and Compliance Services, Wage and Investment Division, at (470) 639-3505.

Sincerely,



Sunita Lough
Deputy Commissioner for
Services and Enforcement

Enclosure

Enclosure

Recommendations for Executive Action

RECOMMENDATION 1

The Commissioner of Internal Revenue should designate a dedicated entity to provide oversight of agency-wide efforts to detect, prevent, and resolve business IDT refund, consistent with leading practices. This may involve designating one business unit as a lead entity, or leveraging cooperative relationships between business units to establish a business IDT leadership team. This entity should have defined responsibilities and authority for managing fraud risk.

COMMENT

We agree with this recommendation and will determine the appropriate oversight structure and scope of authority.

RECOMMENDATION 2

The Commissioner of Internal Revenue should develop a fraud risk profile for business IDT that aligns with leading practices. This should include (1) identifying inherent fraud risks of business IDT, (2) assessing the likelihood and impact of inherent fraud risks, (3) determining fraud risk tolerance, and (4) examining the suitability of existing fraud controls.

COMMENT

We agree with this recommendation and will develop a fraud risk profile for business identity theft (IDT) that aligns with leading practices.

RECOMMENDATION 3

The Commissioner of Internal Revenue should develop, document, and implement a strategy for addressing fraud risks that will be identified in its fraud risk profile.

COMMENT

We agree with this recommendation.

RECOMMENDATION 4

The Commissioner of Internal Revenue should ensure that IRS collects additional data on business IDT by identifying and implementing new fraud filters consistent with its fraud risk profile. This should include prioritizing IDT filters for tax forms determined to be most at risk based on an analysis of risk tolerances.

COMMENT

We agree with this recommendation.

2

RECOMMENDATION 5

The Commissioner of Internal Revenue should identify and implement methods to address delays in resolving business IDT cases due to correspondence-based authentication. This could involve using different methods for taxpayer authentication based on the risk level of the return.

COMMENT

We agree with this recommendation and will complete an analysis on other methods of authentication.

RECOMMENDATION 6

The Commissioner of Internal Revenue should establish customer service-oriented performance goals for resolving business IDT cases.

COMMENT

We will review our customer service-oriented performance goals and modify them, as warranted, to address the resolution of business IDT cases.

Appendix III: GAO Contact and Acknowledgments

GAO Contact

James R. McTigue, Jr. (202)-512-9110 or mctiguej@gao.gov

Staff Acknowledgments

In addition to the contact named above, Shannon Finnegan (Assistant Director), Heather A. Collins (Analyst-in-Charge), Ann Czapiewski, Michele Fejfar, Robert Gebhart, Tonita Gillich, Bethany Graham, James Andrew Howard, Krista Loose, Jungjin Park, Bryan Sakakeeny, and Rebecca Shea made significant contributions to this report.

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 our website. Each weekday afternoon, GAO posts on its [website](#) newly released reports, testimony, and correspondence. You can also [subscribe](#) to GAO's email updates to receive notification of newly posted products.

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, <https://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 [Email Updates](#). Listen to our [Podcasts](#).
Visit GAO on the web at <https://www.gao.gov>.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

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

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@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

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707 U.S. Government Accountability Office, 441 G Street NW, Room 7814, Washington, DC 20548

