United States Government Accountability Office

Report to the Committee on Finance, U.S. Senate

May 2020

EMPLOYMENT-RELATED IDENTITY FRAUD

Improved Collaboration and Other Actions Would Help IRS and SSA Address Risks

Accessible Version

GAO Highlights

Highlights of GAO-20-492, a report to the Committee on Finance, U.S. Senate.

May 2020

EMPLOYMENT-RELATED IDENTITY FRAUD
Improved Collaboration And Other Actions Would Help IRS And SSA Address Risks

Why GAO Did This Study

Employment-related identity fraud poses risks to IRS's ability to collect taxes owed on wages and to SSA's ability to correctly calculate and manage Social Security benefits.

GAO was asked to review employment-related identity fraud. This report examines (1) the potential scope of employment-related identity fraud, including what IRS knows about this type of fraud and what GAO could determine by analyzing Department of Health and Human Services' National Directory of New Hires (NDNH) and IRS data; (2) SSA and IRS actions to detect and deter this fraud as well as notify victims; and (3) SSA and IRS's collaboration on the issue.

GAO analyzed 3 months of 2016 NDNH wage data and 2016 IRS taxpayer data to identify potential employment-related identity fraud. GAO also reviewed relevant IRS and SSA documentation and interviewed agency officials.

This is a public version of a sensitive report that GAO issued in January 2020. Information that SSA deemed sensitive has been omitted.

What GAO Recommends

GAO is making 12 recommendations to IRS and SSA, including that IRS assess the feasibility of adding checks to its review of employment-related identity fraud, and assess the costs and benefits of expanding enforcement; and that both agencies improve the implementation of their MOU. SSA agreed and IRS neither agreed nor disagreed with the recommendations.

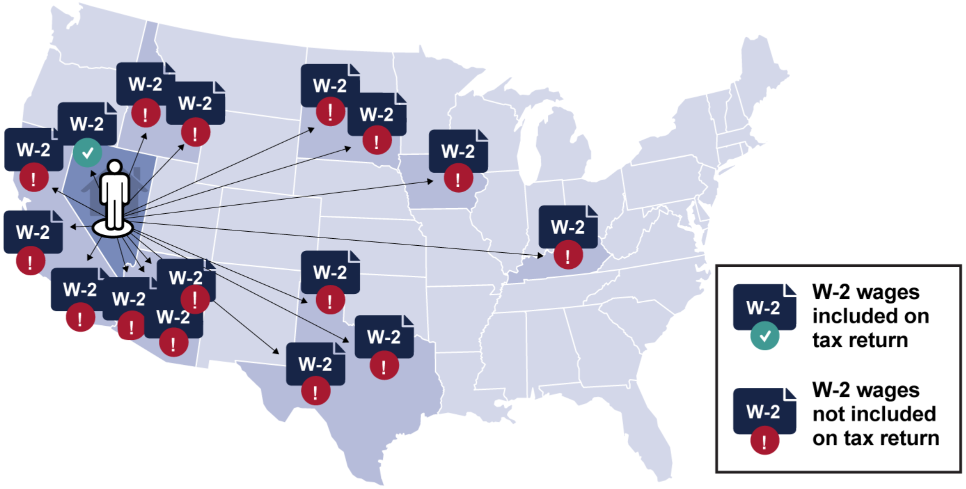
View GAO-20-492. For more information, contact Jessica Lucas-Judy at (202) 512-9110 or LucasJudyJ@gao.gov, or Rebecca Shea at (202) 512-6722 or SheaR@gao.gov.

What GAO Found

Employment-related identity fraud occurs when people use a name or Social Security number (SSN) other than their own to get a job. People may do this if they are not authorized to work in the United States or are trying to avoid child support payments, among other reasons. Victims may face Internal Revenue Service (IRS) enforcement actions based on wages earned by fraudsters. IRS identified more than 818,000 cases in 2018, but this included only one form of employment-related identity fraud—mismatches between the identity listed on the Form W-2, Wage and Tax Statement (W-2) and the identity on the tax return. The true scope of employment-related identity fraud is unknown.

GAO reviewed additional forms of this fraud and identified 1.3 million SSNs that for 2016 had both (1) characteristics associated with employment-related identity fraud; and (2) wages reported by the employer on a W-2, but not reported by the employee on a tax return. This includes about 9,000 individuals whose employers reported W-2s in five or more states, but who did not include them all on their tax return (see figure).

Example of a Social Security Number Potentially Used for Employment-Related Identity Fraud


W-2
W-2 wages included on tax return
W-2 wages not included on tax return

Source: GAO analysis of U.S. Department of Health and Human Services National Directory of New Hires and Internal Revenue Service data. | GAO-20-492

The Social Security Administration (SSA) processes W-2s before sending W-2 data to IRS for enforcement purposes. SSA has developed processes to detect some inaccurate W-2s and notify potential fraud victims. IRS uses W-2 information to deter some potential fraudsters, but has not assessed the costs and benefits of expanding its enforcement efforts to include certain individuals who may underwithhold taxes or not file returns. Doing so could help IRS determine if such an effort would enable the agency to collect additional revenue.

SSA and IRS entered into a memorandum of understanding (MOU) to collaborate to exchange wage data. However, they have not established performance goals and measures for the MOU, implemented the MOU's monitoring provisions, or clearly defined the data elements they exchange.

Contents

Tables

Figures

Abbreviations

AUR	Automated Underreporter
CAWR	Combined Annual Wage Reporting
DHS	Department of Homeland Security
EDCOR	Educational Correspondence
EIN	Employer Identification Number
IDT	Identity Theft
IRS	Internal Revenue Service
ITIN	Individual Taxpayer Identification Number
MOU	Memorandum of Understanding
NDNH	National Directory of New Hires
Numident	Numerical Index File
OIG	Office of the Inspector General
SSA	Social Security Administration
SSN	Social Security Number
SWED	Scrambled Wage Earnings Discrepancy
TIGTA	Treasury Inspector General for Tax Administration
TIN	Taxpayer Identification Number
W-2	Form W-2, Wage and Tax Statement
WHC	Withholding Compliance Program

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

May 6, 2020

The Honorable Charles E. Grassley
Chairman
The Honorable Ron Wyden
Ranking Member
Committee on Finance
United States Senate

Employment-related identity fraud occurs when people use a name or Social Security number (SSN) other than their own to get a job. Individuals may commit employment-related identity fraud for a variety of reasons, including because they are not authorized to work in the United States, are trying to avoid child support payments, or are trying to conceal a criminal record that makes them ineligible for certain employment.

This type of fraud poses risks to the Social Security Administration's (SSA) ability to correctly calculate and manage benefit payments for programs such as Social Security retirement and Supplemental Security Income.[1] It can also lead the Internal Revenue Service (IRS) to incorrectly determine that some individuals failed to report wages and owe taxes. IRS may expend enforcement resources following up with these individuals, only to find that they are victims of employment-related identity fraud.

Employment-related identity fraud can also hurt victims whose names and SSNs are used by others to gain employment. Victims risk being held liable by IRS for unpaid taxes on wages earned by fraudsters, receiving reduced benefit payments from some federal programs, or facing challenges planning for retirement if identity fraud wages are credited to their master earnings records. Further, it can be burdensome for victims to notify IRS and SSA of fraudulent wages, particularly if victims' identities are repeatedly used to commit fraud. Victims may also be at risk of other types of fraud if fraudsters use their identities for other purposes, such as applying for credit.

Although federal agencies have attempted to identify limited instances of employment-related identity fraud, the full scope of employment-related

[1] Officially titled Old-Age and Survivor Insurance, the Social Security retirement program provides benefits to retired workers, their families, and survivors of deceased workers.

identity fraud or its impact on the tax system remains unknown. In 2016, the Treasury Inspector General for Tax Administration (TIGTA) reported that IRS identified almost 1.1 million taxpayers whose names and SSNs were used by employment-related identity fraudsters to obtain jobs between 2011 and 2015.[2] Some fraudsters might obtain employment using combinations of names and SSNs that do not belong to a specific individual listed in SSA's records. In 2013, the SSA Office of the Inspector General (OIG) reported that 100 employers submitted more than 2.3 million Forms W-2, Wage and Tax Statement (W-2) where the employee's name and SSN did not match SSA records; some of these W-2s may be fraudulent.[3]

You asked us to examine the impacts of employment-related identity fraud. This report examines (1) the potential scope of employment-related identity fraud, including what IRS knows about this type of fraud and what we could determine by analyzing the Department of Health and Human Services' National Directory of New Hires (NDNH) and IRS data; (2) SSA actions to detect and deter this fraud as well as notify victims; (3) IRS actions to detect and deter this fraud as well as notify victims; and (4) the extent to which SSA and IRS are collaborating to address the issue.

This report is a public version of a sensitive report that we issued in January 2020.[4] SSA deemed some of the information in our January report as sensitive, which must be protected from public disclosure. Therefore, this report omits sensitive information about SSA's controls for detecting potential employment-related identity fraud. Although the information provided in this report is more limited, the report addresses the same objectives as the sensitive report and uses the same methodology.

To describe and analyze the potential scope of employment-related identity fraud, we identified wage records associated with individuals at risk of identity theft. Specifically, we reviewed relevant TIGTA, SSA OIG, Federal Trade Commission, and our work on SSN misuse to identify

[2] TIGTA, *Processes Are Not Sufficient to Assist Victims of Employment-Related Identity Theft*, 2016-40-065 (Washington, D.C.: Aug. 10, 2016).

[3] SSA OIG, *Employers Who Report Wages with Significant Errors in the Employee Name and Social Security Number*, A-08-12-13036 (Baltimore, MD: Aug. 9, 2013).

[4] GAO, *Employment-Related Identity Fraud: Improved Collaboration and Other Actions Would help IRS and SSA Address Risks,* GAO-20-38SU (Jan. 30, 2020).

characteristics of groups that may be at risk of SSN misuse.[5] To do this, we used SSA's full death file; SSA's Numerical Index File (Numident), SSA's master file of all assigned SSNs; and a 3-month extract of NDNH data to identify SSNs that appeared to belong to individuals who were deceased,[6] elderly (over 84), or children (under 14) or who had three or more wage records between August and October 2016,[7] the oldest data available at the time of our review that aligned with IRS data.

Focusing on these groups of SSNs, we used IRS data to determine the number of SSNs at risk of employment-related identity fraud and possible tax compliance issues. Specifically, we identified SSNs with a wage listed on one or more employer-submitted W-2 that was not reported to IRS on a tax return by the taxpayer. Last, we used tax return data to analyze selected tax characteristics of both groups of individuals we identified as having indicators of employment-related identity fraud as well as those we did not. For example, we analyzed data on wage withholding rates, the

[5] GAO, *Supplemental Security Income: Wages Reported for Recipients Show Indications of Possible SSN Misuse,* GAO-14-597 (Washington, D.C.: July 16, 2014), FTC, *Consumer Sentinel Network: Data Book 2017* (Washington, D.C.: March 2018), SSA OIG, *Improper Use of Elderly Individuals' Social Security Numbers*, A-03-16-24028 (Baltimore, MD: Jan. 3, 2017), and TIGTA, *Efforts Are Resulting in the Improved Identification of Fraudulent Tax Returns Involving Identity Theft*, 2015-40-026 (Washington, D.C.: Apr. 24, 2015).

[6] NDNH is a database of individuals employed in the United States. The database is administered by the Department of Health and Human Services' Office of Child Support Enforcement. NDNH is designed to assist state child support agencies in locating parents and taking appropriate interstate actions concerning child support orders. Some authorized agencies also use NDNH data to help prevent overpayments and detect fraud. For example, IRS has access to NDNH to administer the Earned Income Tax Credit. However, IRS and SSA are not authorized to use NDNH information to detect potential employment-related identity fraud. We were authorized to use NDNH through the GAO Access and Oversight Act of 2017, Pub. L. No. 115-3, 131 Stat. 7.

[7] Based on our analysis of NDNH data, about 98 percent of individuals who earned wages in 2016 had wage records from either one or two employers. Because an employment fraud victim may have an additional wage record for each instance of employment fraud and an individual with three or more wage records is uncommon, we determined these individuals were at risk of employment fraud.

prevalence of select IRS identity theft indicators on taxpayers' accounts, and IRS enforcement actions taken against these individuals.[8]

We assessed the reliability of the SSA full death file, SSA Numident, the Department of Health and Human Services' NDNH quarterly wage data, and select elements of IRS's Compliance Data Warehouse by reviewing relevant documentation, interviewing knowledgeable agency officials, and performing electronic testing to determine the validity of specific data elements in the data. We determined that the data elements used in our analysis were sufficiently reliable for the purpose of our work.

To assess SSA and IRS actions to detect and deter employment-related identity fraud as well as notify victims, we reviewed relevant documentation including IRS's *Internal Revenue Manual* and SSA's *Policy Operations Manual System* and also interviewed knowledgeable agency officials. We compared IRS's and SSA's efforts to relevant *Standards for Internal Control in the Federal Government*.[9] We also assessed the agencies' efforts against IRS's and SSA's respective strategic plans as well as select leading practices to combat fraud, as identified in the *Framework for Managing Fraud Risks in Federal Programs*.[10]

To evaluate the extent to which SSA and IRS are effectively collaborating to address the issue, we reviewed relevant agency documents, such as IRS and SSA's main information sharing agreement, other IRS-SSA legal agreements, meeting minutes from IRS-SSA joint meetings, and policy manuals. We interviewed knowledgeable officials from IRS and SSA, as well as agency officials from the Federal Trade Commission, which assists victims and collects statistics on identity theft. We also interviewed

[8] GAO, *A Framework for Managing Fraud Risks in Federal Programs*, GAO-15-593SP (Washington, D.C.: July 2015). We assessed IRS procedures against the information gathering and data analytics leading practices in the Framework. We did not conduct a comprehensive fraud risk assessment of the IRS enforcement programs. Our assessment was limited to the control activities surrounding employment-related identity fraud. GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 10, 2014).

[9] GAO-14-704G.

[10] GAO-15-593SP. We assessed IRS's and SSA's procedures against the leading practice in the Framework. We did not conduct a comprehensive fraud risk assessment of IRS or SSA programs. Our assessment was limited to the control activities surrounding employment-related identity fraud.

officials at the Department of Homeland Security (DHS) because it helps employers verify the identities of employees. We assessed IRS and SSA's collaboration efforts against leading practices we previously identified for collaboration.[11] Specifically, we identified key elements of each leading practice and assessed the extent to which SSA and IRS collaboration on employment-related identity fraud aligned with leading practices. For a more detailed discussion of our scope and methodology, see appendix I.

The performance audit upon which this report is based was conducted from November 2017 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. We worked with SSA from October 2019 to May 2020 to prepare this public version of the original sensitive report for public release. This public version was also prepared in accordance with these standards.

[11] GAO, *Managing for Results: Key Considerations for Implementing Interagency Collaborative Mechanisms*, GAO-12-1022 (Washington, D.C.: Sept. 27, 2012) and *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, GAO-06-15 (Washington, D.C.: Oct. 21, 2005).

Background

Employment-Related Identity Fraud

Taxpayers may first realize they are victims of employment-related identity fraud when IRS notifies them of discrepancies in the reporting of income earned using their names and SSNs. After filing deadlines have passed, IRS's Nonfiler and Automated Underreporter (AUR) programs use W-2 information to identify and follow up with taxpayers who appear to owe taxes but either have not filed returns (Nonfiler) or have filed returns but underreported earnings (AUR). Other taxpayers may become aware that their SSNs were used by other people when IRS sends them an Employment-Related Identity Theft (CP01E) notice. IRS sends these notices to taxpayers whose SSNs appear on W-2s that have been attached to tax returns (Forms 1040, U.S. Individual Income Tax Return) that were filed with Individual Taxpayer Identification Numbers (ITIN) (see sidebar). In these cases, IRS marks the taxpayer accounts with an employment-related identity theft indicator. Victims may also notice wages they did not earn appearing on their Social Security earnings record or may be alerted by SSA that their Supplemental Security Income benefits are being reduced or eliminated because of wages earned by someone else using their SSN.[12]

Individual Taxpayer Identification Number (ITIN)

An ITIN is a tax processing number issued by IRS to individuals who are required to have a U.S. taxpayer identification number but who do not have and are not eligible to obtain a Social Security number from the Social Security Administration.

IRS issues ITINs to help individuals comply with the U.S. tax laws, and to provide a means to efficiently process and account for tax returns and payments for those not eligible for Social Security numbers.

Source: IRS. | GAO-20-492

Information Exchanges Involved in Employment-Related Identity Fraud

The following individuals and agencies are involved in verifying individuals' eligibility for employment, in processing wage information, or in monitoring identity fraud cases.

- **Employer:** Employers are required to complete the Form I-9, Employment Eligibility Verification for new hires.[13] As part of completing the form, employers certify that they have examined documentation demonstrating that new hires are who they say they are, are eligible for employment, and that the documentation appears

[12] SSA's Supplemental Security Income program makes monthly payments to people who have low income, few resources, and who are either age 65 or older, blind, or disabled. Blind or disabled children may also get Supplemental Security Income.

[13] 8 C.F.R § 274a.2.

to be genuine. The employer is required to submit a W-2 to each employee as well as SSA by January 31 each year.

- **Employee:** As part of obtaining employment, the employee provides the employer with documentation to authenticate his or her identity. It is at this point that the employee could provide someone else's SSN or other information.
- **DHS:** DHS manages E-Verify, a free, internet-based system that employers can use to verify employees' employment eligibility. SSA supports DHS in this effort. Federal agencies are required to use E-Verify for federal employees and contractors.[14] Some states also require employers to use E-Verify to verify the eligibility of some or all employees or contracts. According to DHS, by the end of fiscal year 2019, more than 890,000 employers were enrolled in E-Verify.
- **SSA:** SSA receives W-2s from employers and uses this information to update earnings records and to make determinations about benefits. After receiving and processing W-2s, SSA sends the W-2 information to IRS as part of the Combined Annual Wage Reporting (CAWR) process. SSA also maintains the Social Security Number Verification Service, a free SSN verification program that registered employers can use to verify that employee names and SSNs match SSA's records before they submit W-2s to SSA.[15]
- **IRS:** IRS uses W-2 information to verify tax return information, such as wages, withholdings, and Employer Identification Numbers (EIN), and to enforce tax law.[16] IRS has legal authority to penalize employers $250 for each inaccurate W-2 they submit up to a maximum of $3 million in total penalties per year.[17] In 2013, the SSA

[14] Office of Management and Budget*, Memorandum for the Heads of Departments and Agencies: Verifying the Employment Eligibility of Federal Employees,* M-07-21 (Aug. 10, 2007); See *Amending Executive Order 12989, as Amended,* Exec. Order No. 13465, 73 Fed. Reg. 33,285 (June 6, 2008); Federal Acquisition Regulation; *FAR Case 2007-013, Employment Eligibility Verification*, 73 Fed. Reg. 67,651 (Nov. 14, 2008) (*codified at* 48 C.F.R. pts. 2, 22, 52).

[15] For additional information on this service, see SSA OIG, *Status of the Social Security Administration's Earnings Suspense File*, A-03-15-50058 (Baltimore, MD: Sept. 22, 2015).

[16] Issued by IRS, an EIN is a type of federal Taxpayer Identification Number and is used to identify a business entity.

[17] 26 U.S.C. § 6721(a).

OIG reported that IRS does not routinely penalize employers who consistently submit erroneous or inaccurate wage information.[18]

- **Federal Trade Commission:** It collects and reports to the public aggregated data from self-reported victims of identity fraud. Victims can visit www.IdentityTheft.gov to report identity theft and access resources.

A Million SSNs May Be at Risk of Employment-Related Identity Fraud and Tax Noncompliance, but the Extent of Such Fraud Is Unknown

Our analysis shows that millions of SSNs in NDNH data exhibited risk characteristics associated with employment-related identity fraud in tax year 2016. More than a million of those were also at risk of not meeting all IRS tax return requirements, such as reporting all associated W-2s. However, IRS did not identify all of those noncompliant returns. Further, employment-related identity fraud can diminish tax revenues. IRS's method for tracking employment-related identity fraud likely understates the extent of the problem.

More Than 2.9 Million SSNs in NDNH Data Had Risk Characteristics in Tax Year 2016

We identified more than 2.9 million SSNs that had risk characteristics associated with SSN misuse, and had evidence of employment activity based on our analysis of NDNH verified quarterly wage records for 122.8 million individuals from August to October 2016.[19] The risk characteristics included:

[18] SSA OIG, *Employers Who Report Wages with Significant Errors in the Employee Name and SSN,* A-08-12-13036 (Baltimore, MD: Aug. 9, 2013). In this report, the SSA OIG recommended that SSA continue working with IRS and DHS to develop a coordinated strategy to reduce the growth of inaccurate W-2 submissions. SSA agreed with this recommendation and reported that ongoing efforts such as promoting use of the Social Security Number Verification Service and E-Verify may reduce growth of inaccurate W-2 submissions.

[19] The Department of Health and Human Services has a process for sending SSNs and names from NDNH to SSA for verification. If the information matches, it is included in the quarterly wage verified record file.

- Individuals who had wages reported for three or more employers in the same quarter;
- Individuals who were deceased;
- Individuals under age 14; and
- Individuals over age 84 (see table 1).

Table 1: Social Security Numbers (SSN) with Risk Characteristics Associated with Potential Employment-Related Identity Fraud Identified in the National Directory of New Hires (NDNH), August-October 2016

Risk characteristic	SSNs identified
Individuals with three or more wage records[a]	2,817,341
Deceased	13,617
Children (under 14)	33,856
Elderly (over 84)	65,823
Total[b]	**2,924,837**

Source: GAO analysis of Department of Health and Human Services' NDNH and SSA data. | GAO-20-492

[a]We identified individuals with multiple wage records using the Department of Health and Human Services' NDNH data, deceased individuals using the Social Security Administration's full death file, and children and the elderly using Social Security Administration's Numerical Index System.

[b]The numbers for the categories do not add up to the total because some individuals fall into multiple categories.

We previously reported that the existence of three or more wage records in the same time frame for the same individual indicates possible SSN misuse, which could include employment-related identity fraud.[20] We also previously reported, along with the Department of Justice and SSA OIG, that deceased persons, children, and elderly populations are at risk of identity theft (IDT).[21] Fraudsters may target these groups because they believe there is a lower chance the SSNs are being used for legitimate employment.

- **Individuals with three or more employers within the same quarter.** Our analysis of NDNH data identified millions of SSNs with

[20] GAO-14-597.

[21] See GAO, *Highlights of a Forum: Combating Synthetic Identity Fraud*, GAO-17-708SP (Washington, D.C.: July 26, 2017); U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics, *Victims of Identity Theft, 2014*, NCJ 248991 (September 2015); Social Security Administration, Office of the Inspector General, *Improper Use of Children's Social Security Numbers*, A-03-12-21269 (March 2014); and Social Security Administration, Office of the Inspector General, *Improper Use of Elderly Individuals' Social Security Numbers*, A-03-16-24028 (January 2014).

three or more wage records from August to October 2016. Specifically, of the 122.8 million SSNs included in the data, we found 2.8 million with three or more wage records in the same quarter. Further, we found almost 10,000 of those SSNs had wages reported by 10 or more employers in the same quarter. It is not uncommon for individuals to have second jobs or to change employers. However, when wages are reported by three or more employers for the same calendar quarter, it can indicate potential misuse of an SSN (see table 2).

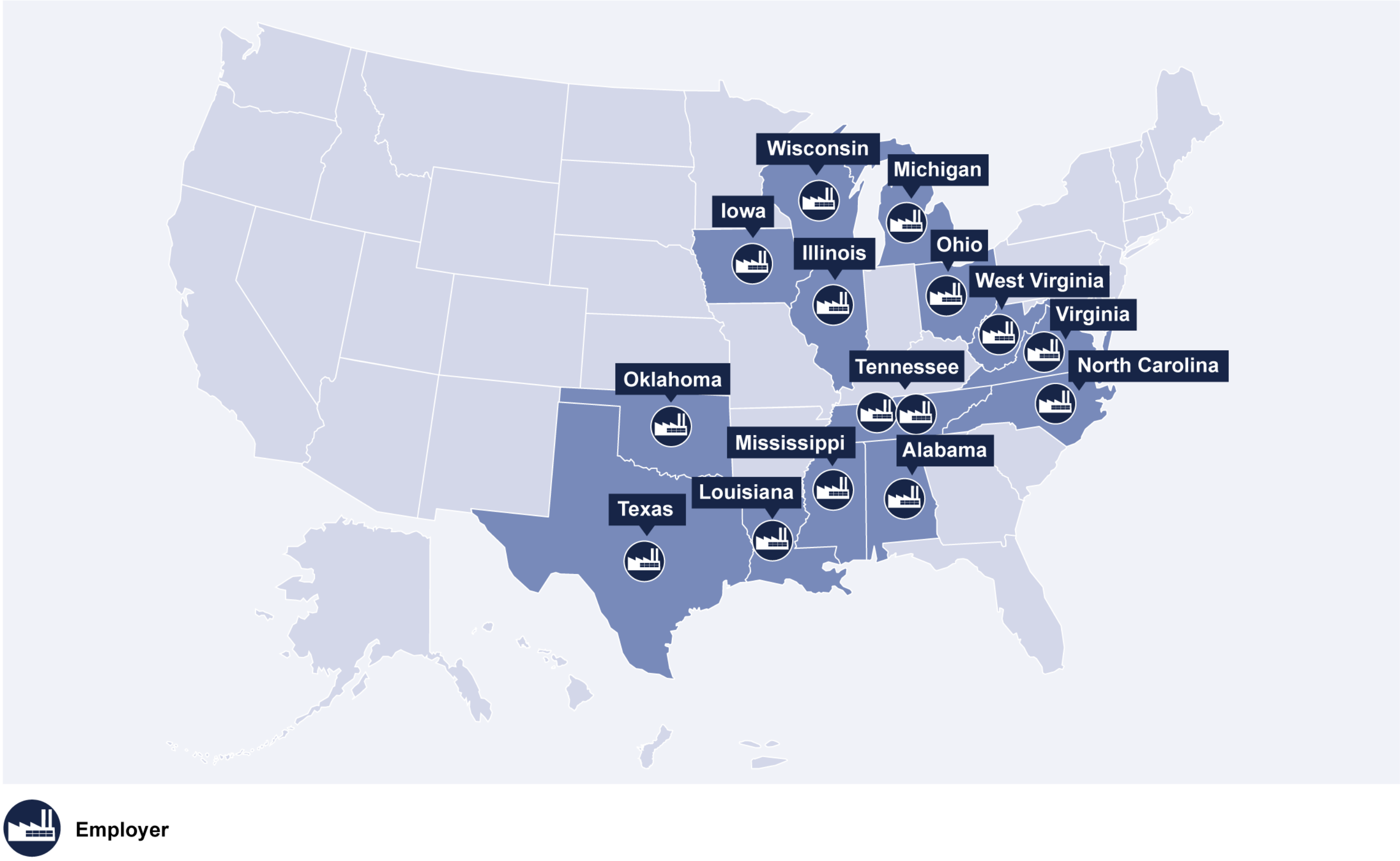
Table 2: Number of Social Security Numbers (SSN) with Three or More Wage Records, August-October 2016

Number of wage records reported by employers	Count of SSN
3	2,265,973
4	386,265
5 to 9	155,190
10 to 19	7,383
20 to 29	2,462
30 or more	68
Total	**2,817,341**

Source: GAO analysis of Department of Health and Human Services' NDNH data. | GAO-20-492

As an illustrative example of potential SSN misuse, one SSN had wages reported by 15 employers from 14 different states for a 3-month period in 2016 (see figure 1). According to the wage data, on average, each of these employers was paying the employee approximately $26,900 a year.

Figure 1: Example of Wage Records for One Social Security Number Reported by 15 Employers in 14 States, August-October 2016



Source: GAO analysis of the U.S. Department of Health and Human Services National Directory of New Hires (data); Map Resources (map). | GAO-20-492

- **Deceased individuals.** We identified several thousand SSNs for deceased individuals included in the NDNH data. Specifically, the NDNH data August-October 2016 showed 13,600 SSNs for individuals SSA identified as deceased prior to May 2016. Of these, 8,400 are reported to have died before 2014. In some cases, we found individuals who had been deceased for a decade.[22]

- **Children.** We identified tens of thousands of SSNs for children under the age of 14. Specifically, NDNH data included 33,856 SSNs of individuals who, according to SSA data, were under the age of 14 with earned income reported. One reason children can be at risk of long-term victimization of employment-related identity fraud is because it usually takes children a while before they start working or applying for financial credit. This gives a fraudster ample opportunity to exploit their stolen identities. Still, there are legitimate circumstances for children to be earning wages, such as in the entertainment and advertising industries.
- **Elderly.** We identified tens of thousands of wage records from elderly individuals. Specifically, the 2016 NDNH data included 65,823 SSNs with earned income reported that SSA data identified as being over 84. The Federal Trade Commission reported that in 2016, approximately one-fifth of IDT complaints they received involved people age 60 years or older. Further, the elderly have low participation rates in the workforce. The Bureau of Labor Statistics reported that, in 2016, the workforce participation rate for those ages 75 and above was 8.4 percent, compared to a rate of 62.8 percent for the overall workforce.[23]

[22] We identified deceased individuals using SSA's full death file. We previously reported on issues with the accuracy and completeness of death data. SSA's procedures for collecting, verifying, and maintaining death reports could result in erroneous or untimely death information. GAO recommended that SSA conduct a risk assessment of its death information processing systems and policies as a component of redesigning its death processing system. SSA completed a risk assessment and a data quality assessment in June 2014 that identified multiple types of errors in the death data. As of October 2019, SSA's redesign efforts are still ongoing. SSA has stated that it is not the custodian of death records, and all users agree to a disclaimer to independently verify death information. As a result, the actual number of deceased individuals with wage records cannot be determined without confirming the reported death information. GAO, *Social Security Death Data: Additional Action Needed to Address Data Errors and Federal Agency Access,* GAO-14-46 (Washington, D.C.: Nov. 27, 2013).

[23] *Civilian labor force participation rate by age, sex, race, and ethnicity*. U.S. Department of Labor, Bureau of Labor Statistics. Accessed June 11, 2019. https://www.bls.gov/emp/tables/civilian-labor-force-participation-rate.htm.

Over a Million SSNs with Risk Characteristics Were Also Associated with Tax Compliance Issues for 2016, Not All of Which Were Pursued by IRS

Some SSNs with risk characteristics were sometimes also associated with IRS returns that did not include required W-2 forms. Specifically, more than 1.3 million individuals—of the 2.9 million SSNs we determined to have risk characteristics associated with SSN misuse—had at least one wage record they did not report to IRS. Of these 1.3 million individuals, more than half failed to include at least one W-2 on their tax return, and slightly less than half (43 percent) did not include any W-2s in a tax return (see table 3).

Table 3: Risk Characteristics Associated with Employment-Related Identity Fraud in Tax Year 2016

Risk characteristic	At least one W-2 not included on tax return	Did not include any W-2s on a tax return	Total Social Security numbers
Individuals with Three or More Wage Records	742,305	512,441	1,254,746
Deceased Individuals	505	11,068	11,573
Children (under 14)	744	19,701	20,445
Elderly (over 84)	839	18,621	19,460
Totals[a]	**743,755**	**557,753**	**1,301,508**

Source: GAO analysis of Department of Health and Human Services' NDNH, SSA, and IRS data. | GAO-20-492

[a] The numbers for the categories do not add up to the total because some individuals fall into multiple categories.

IRS has enforcement tools that are intended to detect reporting deficiencies, but these tools did not always detect the reporting issues we identified. IRS can use Automated Underreporter (AUR) and the Nonfiler, as well as seven IDT-related indicators to mark a taxpayer's account or W-2 if it has determined that the SSN was compromised (see sidebar). We compared data from these enforcement tools and IDT indicators to the 1.3 million individuals identified above and found that IRS did not mark all accounts or W-2s.

IDT-Related Indicators Used by IRS

We reviewed the following ways IRS identifies issues related to employment-related identity fraud.

Four action codes that IRS uses to mark a taxpayer's account:

- Action Code 501: closed identity theft cases initiated by a taxpayer.
- Action Code 506: closed identity theft cases initiated by IRS.
- Action Code 524: deceased taxpayer. It prevents the use of a deceased taxpayer's identity on a federal income tax return.
- Action Code 525: mismatch between the identity listed on the W-2 and on the tax return. These are cases where returns filed with an Individual Taxpayer Identification Number include a W-2 with an SSN belonging to another person.

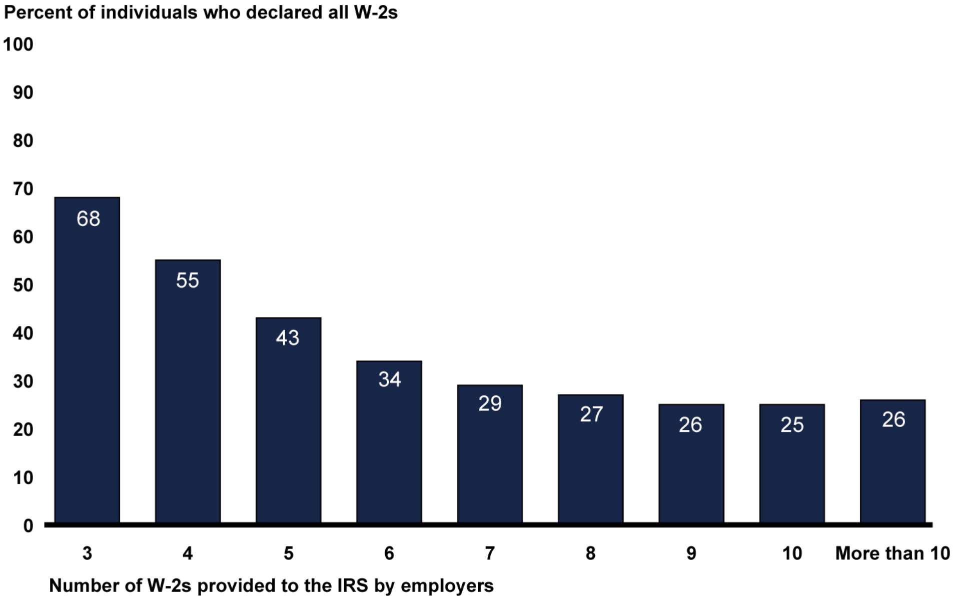
Three codes IRS uses to mark W-2s:

- W-2 credibility code: identifies earnings after death or excessive wages of a young child.
- W-2 suspect employee: identifies suspicious SSNs.
- W-2 suspect employer: identifies suspicious employer identification number.

Source: IRS. │ GAO-20-492

- **Individuals with three or more W-2s for the same period.** More than a million individuals with three or more wage records did not declare at least one W-2. Additionally, we found that, in general, the more W-2s an individual had, the less likely it was that all of them would be reported to IRS (see figure 2). For instance, individuals with three W-2s declared all of them 68 percent of time, while individuals with seven declared all of them 29 percent of the time.

Figure 2: Percentage of Individuals with Three or More W-2s Who Declared All W-2s in Tax Year 2016



Source: GAO analysis of the U.S. Department of Health and Human Services National Directory of New Hires and Internal Revenue Service (IRS) data. | GAO-20-492

Using its enforcement tools, IRS identified some of these individuals with three or more W-2s. Of the 1.25 million individuals in our analysis with three or more wage records who did not include all W-2s in tax year 2016, about 600,000 had wages totaling more than $23,200, meaning that they were required to file a tax return.[24] Of these, about 340,000 individuals had at least one of the seven IDT-related indicators or were pursued through AUR or Nonfiler. In addition, IRS pursued—with AUR or Nonfiler—about half of the nearly 100 individuals who had 50 or more W-2s reported by employers for 2016.[25] In addition, approximately 9,000 individuals with wages totaling more than $23,200 and that did not include all W-2s in tax year 2016 also lived in five or more states (see figure 3 for an illustrative example).

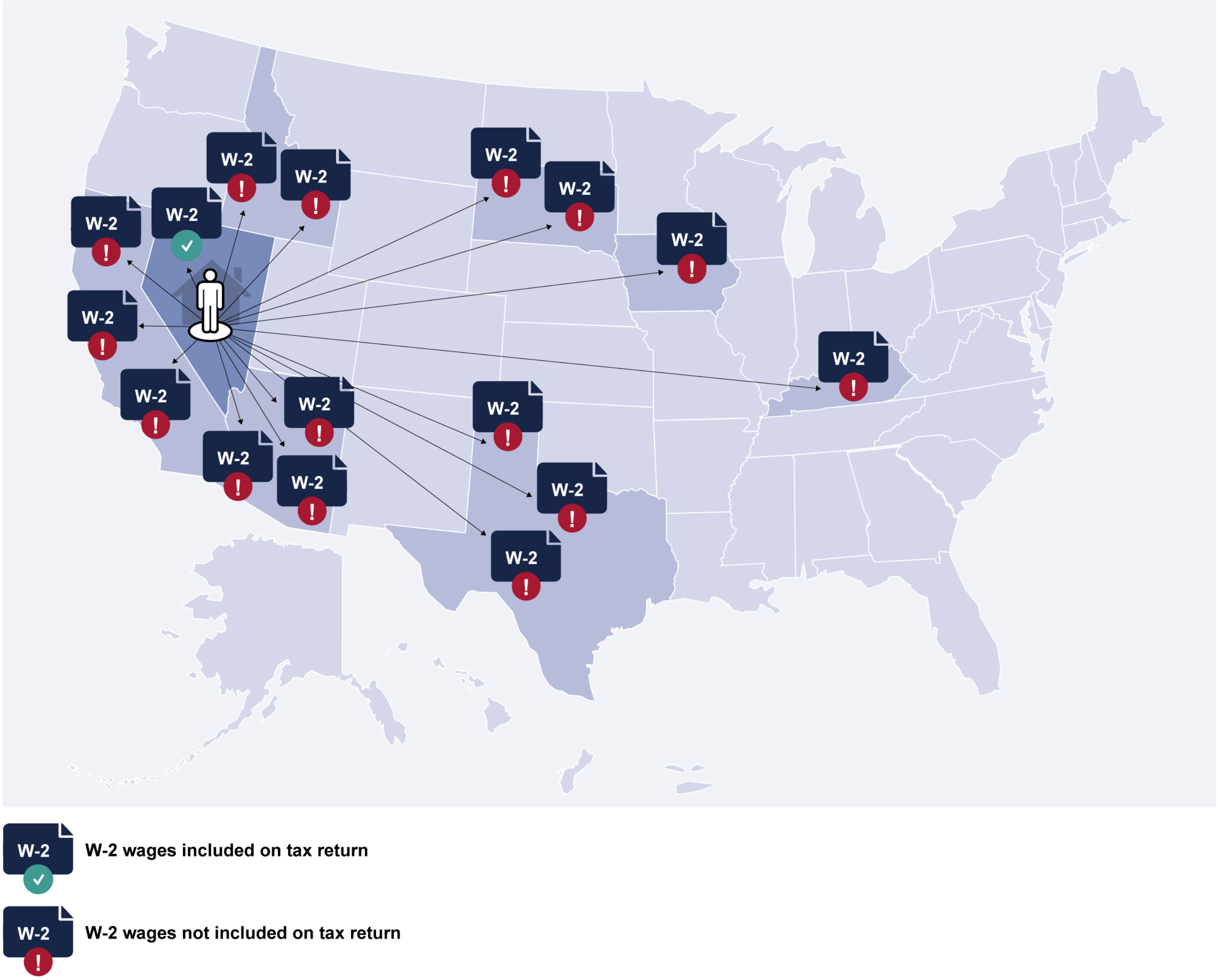
Table data of Figure 2: Percentage of Individuals with Three or More W-2s Who Declared All W-2s in Tax Year 2016

Number of W-2s provided to IRS by employers	Percent of individuals who declared all W-2s
3	68
4	55
5	43
6	34
7	29
8	27
9	26
10	25
More than 10	26

[24] Filing requirements differ for each taxpayer. As a result, we took a conservative approach and compared populations to the highest potential minimum filing requirement for 2016. For the deceased, the elderly, and individuals with three or more wage records, we used the IRS earned income threshold for married filing jointly where both spouses were over age 65, which is $23,200. For children, the earned income threshold was $7,850.

[25] In table 2, we noted 68 SSNs with 30 or more wage records. That number was obtained using NDNH data. The number in this section—100 individuals who had 50 or more W-2s—is different since it was obtained using IRS data and represents W-2 information that employers report to the IRS through SSA.

Figure 3: Example of Social Security Number at Risk of Employment-Related Identity Fraud in 2016 with Multiple W-2s in States Different Than What Was Included on the Tax Return


W-2
W-2 wages included on tax return
W-2 wages not included on tax return

Source: GAO analysis of U.S. Department of Health and Human Services National Directory of New Hires and Internal Revenue Service data. | GAO-20-492

- **Deceased individuals.** IRS did not apply IDT-related indicators to some of the accounts of deceased individuals we identified as having employer-reported wages not included on a tax return. Out of the 11,573 deceased individuals who reported earned income, we identified nearly 2,627 who earned at least $23,200, a threshold requiring the filing of a tax return. Of these, about 2,441 had at least one of the seven IDT-related indicators or were pursued under IRS's AUR or Nonfiler enforcement programs. However, there were still 186 individuals that IRS did not identify.

- **Elderly.** Out of the 19,460 elderly individuals who reported earned income, we identified nearly 3,800 who earned enough to be required to file a tax return. Of these, about 1,700 had at least one out of the seven IDT-related indicators on their account or were pursued under IRS's AUR or Nonfiler enforcement programs. However, there were still about 2,100 individuals that IRS did not identify.
- **Children.** For tax year 2016, individuals under age 14 were only required to file taxes if they earned more than $7,850. However, nearly 1,900 met this filing threshold and failed to include at least one W-2 on their tax returns. Of these, nearly 1,000 had at least one of the seven IDT-related indicators applied to their account by IRS or were pursued under IRS's AUR or Nonfiler enforcement programs. However, there were still about 900 individuals that IRS did not identify.

In considering employment-related identity fraud, IRS focuses on only one of the seven IDT-related indicators. Specifically, IRS considers mismatches between the identity listed on the W-2 and the identity on the tax return as a type of employment-related identify fraud. IRS does not consider other characteristics, such as individuals with multiple wage records, in its checks for employment-related identity fraud. Doing so would require the development of new codes or the modifications of existing ones.

According to the *Fraud Risk Framework*, two leading practices for managing fraud risks include (1) identifying specific tools, methods, and sources for gathering information; and (2) designing and implementing control activities such as data-analytics activities to prevent and detect fraud.[26] IRS addressed these leading practices, in part, through the AUR program, Nonfiler program, and seven IDT-related indicators, but there were still individuals in the population we examined that IRS did not identify. By assessing and documenting the feasibility of incorporating additional checks—such as multiple wage records or wage records for children under 14—into its checks of employment-related identity fraud,

[26] GAO-15-593SP.

IRS may be able to develop a method for identifying additional taxpayers at risk of this type of fraud.

Employment-Related Identity Fraud Can Reduce Tax Revenue

IRS officials stated that employment-related identity fraud has limited tax consequences, as employees will nonetheless pay required taxes—including federal, state, and payroll taxes—through payroll withholding even if the fraudster fails to file a tax return. However, we found that federal income tax withholding was lower for SSNs that did not declare all the W-2s than for SSNs with all W-2s reported (see table 4).

Table 4: Federal Income Tax Withholdings for Social Security Numbers (SSN) at Risk of Employment-Related Identity Fraud in 2016

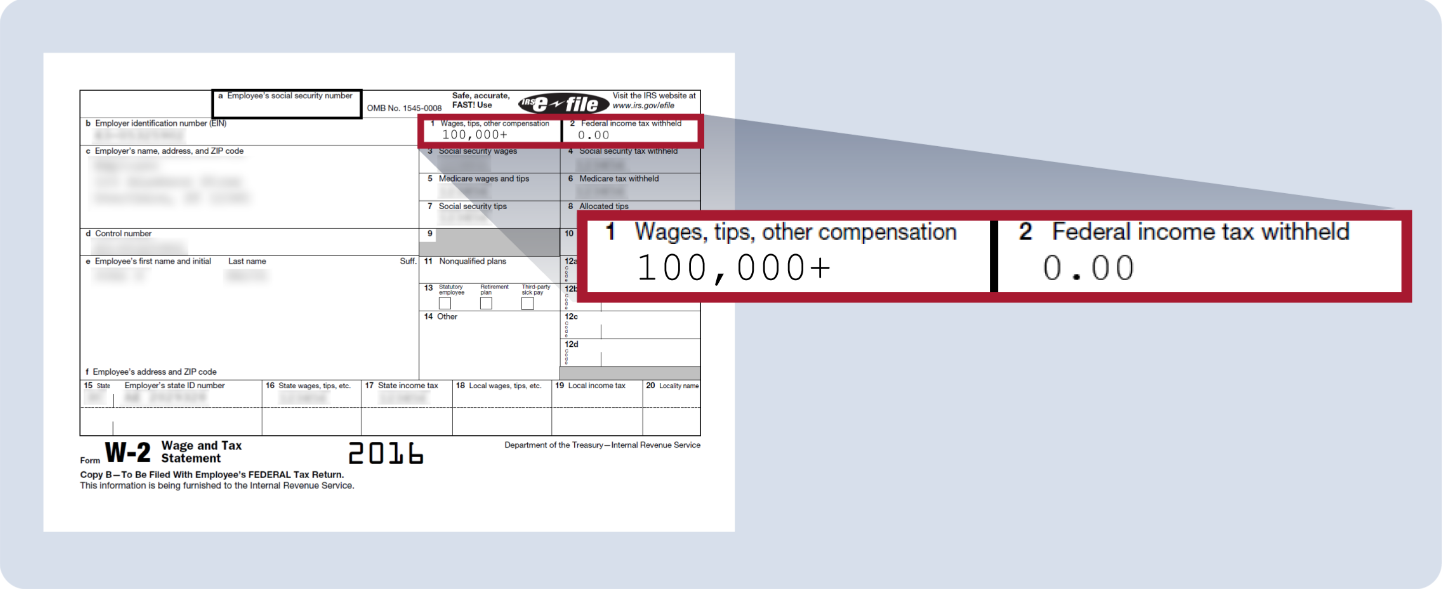
Categories	Number of individuals	Average withholdings (dollars)	Number of individuals with zero withholdings
SSNs where all W-2s were accounted for on a tax return	1,539,243	7,227	26,350
SSNs that had at least one W-2 that was not accounted for on a tax return	743,755	4,116	7,740
SSNs that did not report any W-2 on a tax return	557,753	3,588	30,128

Source: GAO analysis of Internal Revenue Service data. | GAO-20-492

Additionally, we found individuals who did not withhold any federal income taxes across all of their related W-2s in 2016. Specifically, 37,868 individuals had at least one W-2 not declared on a tax return and withheld no federal income tax over the course of the year. Together, these individuals earned approximately $340 million in 2016.

Further, 18 W-2s that were not reported on a tax return showed wages earned of more than $100,000 yet had $0 of federal income tax withheld (see figure 4 for example).

Figure 4: W-2 with Zero Federal Income Tax Withheld That Was Not Declared on a Tax Return for 2016 for a Social Security Number at Risk of Employment-Related Identity Fraud



a Employee's social security number

OMB No. 1545-0008

Safe, accurate, FAST! Use IRS e-file

Visit the IRS website at www.irs.gov/efile

b Employer identification number (EIN) [redacted]

c Employer's name, address, and ZIP code [redacted]

d Control number [redacted]

e Employee's first name and initial [redacted] Last name [redacted] Suff.

f Employee's address and ZIP code

1 Wages, tips, other compensation 100,000+

2 Federal income tax withheld 0.00

3 Social security wages [redacted]

4 Social security tax withheld [redacted]

5 Medicare wages and tips [redacted]

6 Medicare tax withheld [redacted]

7 Social security tips [redacted]

8 Allocated tips

9

10

11 Nonqualified plans

12a Code

12b Code

12c Code

12d Code

13 Statutory employee □ Retirement plan □ Third-party sick pay □

14 Other

15 State [redacted] Employer's state ID number [redacted]

16 State wages, tips, etc. [redacted]

17 State income tax [redacted]

18 Local wages, tips, etc.

19 Local income tax

20 Locality name

Form W-2 Wage and Tax Statement 2016

Department of the Treasury—Internal Revenue Service

Copy B—To Be Filed With Employee's FEDERAL Tax Return.
This information is being furnished to the Internal Revenue Service.

1 Wages, tips, other compensation 100,000+

2 Federal income tax withheld 0.00

Source: GAO analysis of U.S. Department of Health and Human Services National Directory of New Hires and Internal Revenue Service data. | GAO-20-492

IRS's Code for Tracking Employment-Related Identity Fraud Likely Understates the Extent of the Problem

Of the indicators IRS uses to track IDT, the only action code that directly relates to employment is Action Code 525, "Employment-related Identity Theft." IRS applies the code to a taxpayer's account when IRS processes a return filed by an individual with an Individual Taxpayer Identification Number (ITIN), and the return includes a W-2 with an SSN that does not belong to the person identified on the ITIN return. IRS refers to this situation as an ITIN/SSN mismatch. In 2018, IRS marked 818,097 accounts with Action Code 525.

IRS officials acknowledged that forms of employment-related identity fraud, other than that captured by Action Code 525, are likely, but they said they do not systematically track these situations for several reasons. First, unless a taxpayer contacts IRS to say he or she did not earn the wages and disclaims them, the agency does not know whether a suspected case is employment-related identity fraud or someone who may not have included legitimate wages on his or her tax return. Second, IRS may be unable to distinguish between employment-related identity fraud and fabricated W-2s for jobs that were not worked (i.e., fake employees of a fake business).[27] Third, while our analysis shows that employment-related identity fraud may be a more widespread problem than the ITIN/SSN mismatch that IRS currently tracks, IRS officials told us that other types of employment-related identity fraud would be identified and addressed through processes the agency applies broadly to all taxpayers, such as the AUR or Nonfiler programs.

For example, according to IRS officials, if IRS receives a fraudulent W-2 from an employer using a legitimate taxpayer's SSN, AUR or the Nonfiler program will detect it as IRS matches W-2s with tax returns. However, our analysis of NDNH and IRS data described earlier in this report shows that there are potential cases that these IRS enforcement programs did not identify.

Standards for Internal Control in the Federal Government states that management should use quality information that is appropriate and complete to achieve the entity's objectives, and that it should communicate quality information externally.[28] However, our analysis of SSNs at risk of employment-related identify fraud indicates that the count of cases that IRS identifies under Action Code 525 likely understates the universe of employment-related identity fraud. By modifying the title of its employment-related IDT action code to more accurately reflect the data covered by the code, IRS can ensure that the agency is appropriately conveying the risk this specific type of employment-related identity fraud poses both to victims and tax administration without suggesting its statistics cover other types of employment-related identity fraud.

SSA Is Taking Steps to Better Detect Inaccurate W-2s and Notify Potential Fraud Victims, but

[27] In July 2018, we reported that IRS was developing rules, models, and filters to detect noncompliance and fraud in business and partnership returns. According to IRS, identity thieves have long used stolen business information to create and file fake W-2s along with fraudulent individual tax returns. However, identity thieves are now using this information to file fraudulent business returns. In May 2018, IRS reported a sharp increase in the number of fraudulent business and partnership returns in recent years. 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).

[28] GAO-14-704G.

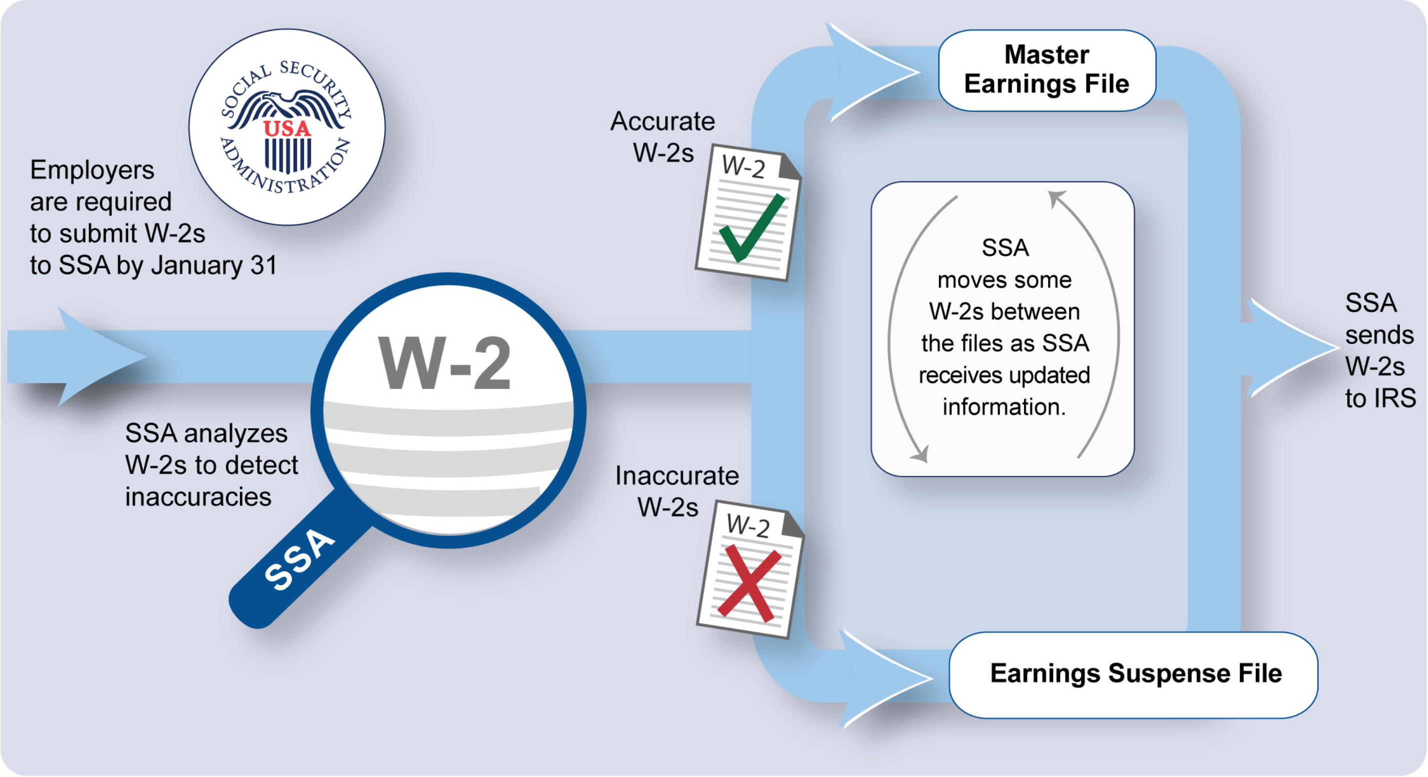
Faces Challenges Addressing Risks Associated with Some Victims

SSA Detects Inaccurate W-2s and Monitors the Effectiveness of W-2 Accuracy Checks

As illustrated in figure 5, SSA analyzes W-2s to detect inaccuracies. For W-2s determined to be accurate, SSA adds wages to the individual's record on the Master Earnings File, a database that SSA uses to determine an individual's eligibility for Social Security benefits and the amount of benefits paid. For W-2s determined to be inaccurate, SSA posts the wage information to the Earnings Suspense File. Inaccurate W-2s may be attributable to various reasons, including employment-related identity fraud or administrative errors.[29]

[29] Details on specific characteristics of inaccurate W-2s were omitted because SSA deemed this information to be sensitive.

Figure 5: SSA Analyzes Forms W-2, Wage and Tax Statement (W-2) to Detect Inaccuracies


Employers are required to submit W-2s to SSA by January 31
SOCIAL SECURITY ADMINISTRATION
USA
W-2
SSA
SSA analyzes W-2s to detect inaccuracies
Accurate W-2s
W-2
Inaccurate W-2s
W-2
Master Earnings File
SSA moves some W-2s between the files as SSA receives updated information.
Earnings Suspense File
SSA sends W-2s to IRS

Source: GAO analysis of Social Security Administration (SSA) information. I GAO-20-492

Note: This figure does not include information on SSA’s controls for detecting W-2 inaccuracies because SSA deemed it sensitive.

SSA receives hundreds of millions of W-2s each year. SSA analyzes incoming W-2s to detect inaccuracies and adds inaccurate W-2s to the Earnings Suspense File. Based on SSA data from tax year 2016, SSA added millions of W-2s to the Earning Suspense File. On a daily basis, SSA electronically forwards IRS W-2s that it has analyzed, including both accurate and inaccurate W-2s.

SSA monitors the effectiveness of its checks for inaccurate W-2s by testing its software prior to the filing season. Prior to each filing season, SSA creates test data that have characteristics of inaccurate W-2s. SSA then processes these data through the annual wage reporting software to ensure automated checks identify potentially inaccurate W-2s according to SSA’s criteria. SSA also has an electronic reporting system in place that SSA employees can use to identify and document problems for management throughout the year. SSA officials told us they have not identified any problems that have prevented checks from working as intended.

This public report omits information that SSA has deemed sensitive related to (1) SSA's efforts to improve W-2 accuracy checks, and (2) SSA's challenges in addressing risks associated with employment-related identity fraud.

SSA Is Taking Steps to More Effectively Communicate Relevant Information to Both Victims and Employers

SSA is taking steps to more effectively communicate to both victims and employers information on potentially inaccurate W-2s, including potential employment-related identity fraud W-2s. When SSA detects a potentially inaccurate W-2, SSA may send a letter to the employer or employee listed on the W-2 that notifies them of the potential inaccuracy. SSA first sends letters to employers. Responses can help SSA resolve inaccuracies by identifying correct wage earners. Responses can also support SSA's efforts to provide taxpayers with correct benefits. SSA sends different letters to employees and employers depending on the type of potential inaccuracy detected:[30]

- **Mismatched name and SSN**. In March 2019, SSA resumed sending Educational Correspondence (EDCOR) letters to employers who submitted W-2s electronically, notifying them of the number of W-2s they electronically submitted with mismatched names and SSNs. The letters request that employers use SSA's Business Services Online portal to view specific names and SSNs that did not match and provide necessary Form W-2C corrections.[31] According to SSA, EDCOR letters are meant to educate employers about mismatches and help SSA post wages to correct earnings records.

  SSA officials told us that SSA had mailed about 577,000 EDCOR letters for electronically submitted W-2s as of June 2019 since resuming the process. Officials said the agency also began sending EDCOR letters for W-2s submitted on paper beginning in October 2019. SSA previously sent EDCOR notices from 1994 through 2007,

[30] Information on SSA's procedures for notifying employers when an SSN belongs to a deceased person or a young child has been omitted because SSA deemed it sensitive.

[31] SSA's Business Services Online portal allows employers and SSA to exchange information over the internet. Employers may use the portal, for example, to electronically send W-2s to SSA and verify that employees' names and SSNs match SSA records.

but SSA stopped sending these notices in response to litigation surrounding a proposed DHS regulation that would have required employers to follow a prescribed course of action upon learning of an employee name or SSN mismatch. DHS rescinded its proposed rule in October 2009. SSA officials told us the agency decided to resume sending EDCOR notices in 2019 because employers are using Business Services Online to file more W-2s electronically. Therefore, employers may be more familiar with the system used to submit W-2C corrections.

SSA has taken action to improve the effectiveness of EDCOR letters since the letters were discontinued in 2007. In 2008, the SSA OIG reported that EDCOR letters were not effective in either communicating wage-reporting problems to employers or identifying correct wage earners.[32] For example, the OIG found that 74 percent of employers who reported W-2s with mismatched names and SSNs did not receive letters. Most employers that did not receive letters submitted 10 or fewer mismatched W-2s whereas SSA only sent letters to employers that submitted more than 10 mismatched W-2s. SSA officials told us that EDCOR letters sent beginning in 2019 are sent to every employer who submits a W-2 with a mismatched name and SSN.

- **Disclaimed wages.** When an individual disclaims wages, SSA staff have the option of sending a letter to the employer who paid the wages to attempt to identify the wage earner. In 2008, the SSA OIG found that SSA seldom sent letters to employers, and recommended that SSA consider generating a standard, annual letter to each employer that submitted a W-2, which was later disclaimed.[33] SSA officials told us that, as of May 2019, SSA staff in all SSA region offices routinely send letters to employers notifying them of disclaimed wages. SSA officials reported the agency sent 20,945 letters in fiscal year 2018.

[32] SSA OIG, *Effectiveness of Educational Correspondence to Employers*, A-03-07-17105 (Baltimore, MD: Dec. 15, 2008).

[33] SSA OIG, *Social Security Number Misuse for Work and the Impact on the Social Security Administration's Master Earnings File*, A-03-07-27152 (Baltimore, MD: Sept. 29, 2008).

IRS Has Not Assessed Opportunities to Expand Detection and Deterrence Activities

IRS's Use of Nonfiler to Detect and Deter Employment-Related Identity Fraud Is Limited

IRS uses relevant information to detect inaccurate W-2s, including potentially fraudulent W-2s, and makes this information available to relevant enforcement programs, including Nonfiler, which IRS uses to follow up with individuals who appear to owe taxes but have not filed.

IRS detects inaccurate W-2s using the results of SSA's annual wage reporting checks and its own efforts to reconcile and correct some inaccuracies. As part of this process, IRS receives Earnings Suspense File W-2s that have mismatched names and SSNs from SSA and attempts to locate the wage earner's correct name and SSN. IRS does so by identifying previously filed tax returns that list the same address as the mismatched W-2s. IRS then compares the names and SSNs listed on W-2s to those on the tax returns to identify accurate name and SSN combinations.

Accurate and inaccurate W-2s are then made accessible to IRS enforcement programs, including Nonfiler. Nonfiler and other programs that support IRS's efforts to collect taxes owed from wage earners, including potential employment fraudsters, also may deter fraudulent activity by reducing the likelihood fraudsters succeed in not paying taxes owed.[34]

In reviewing IRS actions that may help deter employment-related identity fraud, we found that Nonfiler uses W-2 information to identify and follow up with individuals who appear to owe taxes but did not file required returns. However, we also found that IRS's use of Nonfiler to collect taxes owed by potential employment fraudsters is limited. Nonfiler is capable of addressing cases involving certain types of employment-related identity fraudsters who appear to owe taxes—specifically fraudsters for whom IRS receives W-2s that have mismatched names and SSNs as well as SSNs associated with deceased persons or children. However, the

[34] We have previously reported that efforts to detect and address potential fraudulent activity deter fraudsters. See GAO-15-593SP.

agency has made limited use of Nonfiler to collect taxes owed on such cases and faces the following resource challenges in doing so:

- **Reduced staffing capacity.** IRS determines the number of noncompliance cases pursued by its enforcement programs based on available resources. IRS's budget declined by about $2.1 billion (15.7 percent) from fiscal years 2011 through 2018 after adjusting for inflation, and corresponding staff reductions have been most significant within IRS enforcement programs, such as Nonfiler.[35] In 2018, the Treasury Inspector General for Tax Administration (TIGTA) reported that resource constraints have left IRS with fewer resources to work cases involving individuals who do not respond to nonfiler notices. For example, TIGTA found that IRS created 430,000 new compliance cases in fiscal year 2017 involving individuals who did not respond to nonfiler notices compared to 1.6 million in fiscal year 2013.[36]
- **Competing priorities.** IRS is focusing its resources on modernizing its information technology systems and implementing Public Law 115-97—commonly referred to as the Tax Cuts and Jobs Act. This law was enacted in December 2017 and included significant changes to corporate and individual tax law.
- **Costly follow-up contacts.** According to IRS officials, collecting taxes owed by employment-related identity fraudsters typically requires IRS staff to make in-person contact with taxpayers by locating them at their places of work, which is resource intensive. According to IRS, in-person contact is typically required because employment fraudsters are unlikely to provide employers and IRS accurate address information on W-2s; therefore IRS often lacks information needed to reach employment fraudsters through mailed Nonfiler notices.

[35] GAO, *Internal Revenue Service: Strategic Human Capital Management is Needed to Address Serious Risks to IRS's Mission*, GAO-19-176 (Washington, D.C.: Mar. 26, 2019). We found that staff reductions in IRS enforcement programs declined by 27 percent from fiscal years 2011 through 2017.

[36] TIGTA, *Trends in Compliance Activities Through Fiscal Year 2017*, 2018-30-069 (Washington, D.C.: Sept. 13, 2018).

IRS Has Not Assessed Opportunities to Expand Activities That May Deter Some Fraudsters Who Underwithhold

To help reduce the number of nonfilers and underreporters, IRS uses the Withholding Compliance Program (WHC) to pre-emptively identify taxpayers who appear to be substantially underwithholding taxes based on prior year W-2 and other information. Through this program, IRS issues "lock-in letters" to employers of individuals who appear to be underwithholding. Lock-in letters require employers to adjust employees' withholding amounts to rates specified by IRS rather than the employees. IRS adjusts withholding rates based on the number of withholding allowances IRS determines the taxpayer is entitled to claim. Employees are also sent lock-in letters informing them of changes to their withholding rates.

WHC may be a more cost-effective opportunity than Nonfiler for IRS to collect appropriate taxes from those employment-related identity fraudsters who do not otherwise file returns and pay taxes owed.[37] First, WHC lock-in letters would be more likely to reach their intended recipients, making them potentially more effective in obtaining their intended responses. IRS sends lock-in letters to employers, and IRS officials said the agency typically has accurate address information for employers. IRS also sends notices to employees affected by lock-in letters, but these letters do not request or require taxpayer action.

Second, businesses that employ employment-related identity fraudsters may be more likely to comply with lock-in letters than fraudsters would to Nonfiler notices. According to a 2018 TIGTA report, compliance with lock-in letters could further be improved if IRS took action against employers who do not comply with the letters and adjust employees' withholdings accordingly.[38] TIGTA recommended that IRS penalize employers who do not respond. IRS has agreed to consider penalties, and officials told us the agency is evaluating opportunities to do so.

[37] In 2018, we reported IRS's estimated costs for different types of interactions with taxpayers. See GAO, *Identity Theft: IRS Needs to Strengthen Taxpayer Authentication Efforts*, GAO18-418 (Washington, D.C.: June 22, 2018).

[38] TIGTA, *Improvements Are Needed in the Withholding Compliance Program*, 2018-30-072 (Washington, D.C: Sept. 20, 2018).

Third, we have previously reported that IRS is less likely to collect taxes owed the longer it takes IRS to contact taxpayers.[39] Therefore, it is likely more effective for IRS to use WHC to address potential tax liabilities before they accrue, rather than use Nonfiler to assess and attempt to contact fraudsters and collect taxes owed months after filing deadlines have passed.

According to IRS officials, WHC issues lock-in letters to address underwithholding by some employees who use matching names and SSNs; however, the program does not issue lock-in letters for cases involving W-2s with mismatched names and SSNs because of privacy concerns. IRS officials said the agency has an obligation to protect all taxpayers, including potential employment-related identity fraudsters. IRS officials told us that IRS previously sent lock-in letters for cases involving mismatched names and SSNs but stopped in 2012 because the agency wanted to avoid potentially disclosing an employment-related identity fraudster's identifying information, such as the names of their employers, to those individuals whose SSNs were used to commit employment fraud.

However, IRS could also redact personally identifiable information in the lock-in letters as it already does this when mailing tax return transcripts.[40] For example, in response to data privacy concerns, in September 2018 IRS began including just the first four characters of business names on tax return transcripts requested by taxpayers. This approach could also be used for sending lock-in letters to employees to reduce disclosures of personally identifiable information in instances where lock-in letters do not reach their intended recipients.

IRS officials told us that WHC's limited resources prevent the program from addressing all underwithholding cases currently identified by the program. Officials also said that, for that reason, expanding WHC to include cases with mismatched names and SSNs would not result in WHC selecting additional cases. However, by not including cases with mismatched names and SSNs, IRS may be missing an opportunity to identify and select a population of underwithholding cases that could lead to greater revenue collection. This is because some cases with

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

[40] An individual's tax return transcript for a particular year shows most line items reported on the individual's tax return for that year. Taxpayers may contact IRS and request IRS send them tax return transcripts either online or by mail at no charge.

mismatched names and SSNs may have greater underwithholding than those cases that are currently selected by WHC.

If IRS were able to allocate more resources toward generating additional lock-in letters in the future, these potential benefits could also increase. In addition, WHC may be more affordable than other enforcement programs to administer on a case-by-case basis because unlike enforcement cases initiated through Nonfiler, WHC does not result in IRS pursuing taxpayers through progressively more costly methods of contact to collect additional revenue. IRS officials acknowledged this possibility and told us the agency has not assessed the potential costs and benefits of expanding WHC to include cases with mismatched names and SSNs.

Internal control standards state that federal managers should use quality information to achieve their objectives, communicate relevant information throughout the agency, and both assess and address risks to their mission.[41] Additionally, leading practices in managing fraud risks include considering the benefits and costs of controls for addressing fraud-related risks.[42] Further, IRS's Strategic Plan has goals to use data analytics to inform decision making and protect the integrity of the tax system.[43]

Because IRS has not evaluated and documented the costs and benefits of expanding WHC to address risks posed by employment-related identity fraudsters, the agency cannot determine whether or not expanding WHC to include mismatch cases would enable IRS to collect additional revenue and deter employment fraud. By conducting such an assessment, IRS could determine whether expanding WHC to include mismatch cases would likely enable IRS to collect additional revenue and deter employment fraud.

IRS's Approach to Managing Impacts on Victims Creates an Enforcement Gap

To manage the impacts of employment-related identity fraud on victims, IRS limits the circumstances under which these victims may be selected

[41] GAO-14-704G.

[42] GAO-15-593SP

[43] Internal Revenue Service, *Strategic Plan: FY2018—2022* (Washington, D.C.: May 23, 2018).

by enforcement programs. In analyzing IRS data, we found about 3 million taxpayers who have either been identified as “employment-related identity theft” victims by IRS (Action Code 525) or who have identified themselves as victims to IRS (Action Code 501). Automated Underreporter (AUR) programming prevents these taxpayers from being selected due to wage discrepancies.[44] Instead, AUR analyzes these taxpayers for reporting discrepancies for other income types, such as investment income.

IRS officials told us excluding these taxpayers from AUR’s W-2 checks helps IRS avoid burdening some victims who may be otherwise selected based on wages earned by a fraudster using the taxpayers’ name and SSN. Selected victims would be required to follow up with IRS to avoid being assessed tax liabilities. Following up would be particularly burdensome for victims whose names and SSNs are used by fraudsters year after year.

Taxpayers with IDT action codes on their accounts are eligible for analysis and selection by other enforcement programs based on discrepancies in W-2 reporting; however, these programs’ low selection rates suggest that it is unlikely IRS will follow up with these victims and notify them of these discrepancies. For example, although Nonfiler analyzes these taxpayers for evidence of income indicating a filing requirement, TIGTA found that IRS notified just 25,105 or 14 percent of all 179,878 nonfiler cases identified in fiscal year 2016 of these discrepancies.[45] Likewise, although IDT victims may be selected for examination, IRS data show that the agency examined about 892,000 or 0.6 percent of all individual income tax returns in fiscal year 2018, the most recent year for which data are available.

IRS officials acknowledge that some of the approximately three million taxpayers with Action Codes 501 or 525 may underreport their own incomes, and excluding these taxpayers from AUR’s W-2 discrepancy checks creates an enforcement gap, enabling some victims who actually

[44] AUR also excludes taxpayers from being selected for discrepancies in W-2 reporting for a given tax year if SSA notifies IRS that SSA has identified the W-2 SSN as “suspect.” Suspect wages include wages that require additional investigation as determined by SSA. We do not focus on IRS’s treatment of taxpayers with suspect wages in our review because these wages are not specific to identity fraud.

[45] TIGTA, *A Significantly Reduced Automated Substitute for Return Program Negatively Affected Compliance and Filing Compliance*, 2017-30-078 (Washington, D.C.: Sept. 29, 2017).

underreported their own wages to avoid enforcement. IRS does not know how many of these taxpayers have underreported wage income.

However, some IDT victims excluded from AUR's wage discrepancy checks may be incentivized to underreport wages and pay less tax than they owe if they learn IRS is unlikely to hold them accountable for paying those taxes. Individuals could learn about this enforcement gap, for example, if they accidentally failed to report wages from an employer and were not later contacted by IRS. In addition other taxpayers may be incentivized to falsely claim they are IDT victims to take advantage of this enforcement gap. In its research into behavioral insights, IRS has found that taxpayers are more likely to be noncompliant when they perceive doing so can yield substantial benefits with minimal costs.[46] We have also previously reported that the extent to which taxpayers misreport income closely aligns with IRS's ability to detect such noncompliance.[47]

In some instances, IRS has information needed to distinguish wages earned by legitimate taxpayers from those potentially earned by employment-related identity fraudsters using that same taxpayer's name and SSN. For example, IRS can reasonably conclude the legitimate taxpayer earned the wages if they are reported on a current- or prior-year return filed by the taxpayer, as this indicates the taxpayer attests to having worked for the employer who paid the wages.

Because IRS excludes IDT victims from AUR's W-2 discrepancy checks, IRS may not identify or collect taxes owed by some who unintentionally underreport their wages (e.g., by forgetting to include a W-2 from a second employer). In addition, IRS is missing an opportunity to incentivize taxpayers to accurately report their income and avoid intentional underreporting.

As previously stated, federal internal control standards call for managers to both use quality information and respond to risks. According to IRS officials, modifying AUR to effectively identify the underreporting of wages actually earned by identity theft victims would require IRS to not only adjust AUR to include wage discrepancy checks for these taxpayers but also to change how AUR identifies wage discrepancies. IRS officials told us that when AUR evaluates a taxpayer's wage information for

[46] IRS, *Behavioral Insights Toolkit* (Washington, D.C.: Jan. 31, 2017).

[47] GAO, *Tax Gap: IRS Needs Specific Goals and Strategies for Improving Compliance*, GAO-18-39 (Washington, D.C.: Oct. 31, 2017).

discrepancies, the program evaluates taxpayers based on aggregated W-2 information. AUR is not programmed to evaluate taxpayers by analyzing some of their W-2s but not others, such as potential employment fraud W-2s.

IRS officials told us modifying AUR to include W-2 discrepancy checks of these taxpayers while excluding potentially fraudulent W-2s would not be a cost-effective use of IRS resources at this time. Specifically, officials noted that AUR discrepancy checks are programmed in the legacy assembly language code, a low-level computer language initially used in the 1950s. Although they were unable to provide an estimate for the costs of modifying this code, IRS officials said the effort would be resource intensive.

IRS is modernizing outdated information technology systems, and officials said it would be more cost effective for the agency to modify W-2 discrepancy checks once the assembly language is replaced. IRS plans to retire 75 percent of the agency’s legacy assembly language code and Common Business-Oriented Language code legacy by the end of fiscal year 2024.[48] Officials told us the agency does not have a specific timeline in place for updating the assembly code that supports AUR, though doing so is a program goal.

Modifying AUR to include wage discrepancy checks for IDT victims as part of IRS’s broader effort to update AUR’s programming code would enable IRS to avoid making costly and redundant changes to legacy coding that IRS plans to replace. It would also be consistent with a goal outlined in IRS’s Strategic Plan to advance the use of data and analytics to inform decision making and could potentially result in IRS collecting additional revenue by enabling IRS to analyze wage information for about three million additional taxpayers to identify any wage reporting discrepancies.[49] Some of these taxpayers may have greater revenue collection potential than cases AUR would otherwise select.

[48] IRS, *IRS Integrated Modernization Business Plan*, (Washington, D.C.: Apr. 18, 2019).

[49] IRS, *Strategic Plan: FY2018—2022*.

SSA and IRS Share Wage Reporting Data, but Opportunities Exist to Improve Collaboration

SSA and IRS Collaborate on Combined Annual Wage Reporting with Defined Roles and Responsibilities

SSA and IRS both have responsibility for parts of the Combined Annual Wage Reporting (CAWR) process to exchange W-2 information between the two agencies and to help ensure that taxpayers report and pay the proper amount of taxes on their wages. The CAWR Memorandum of Understanding (MOU), which was signed in 2007, is a key part of their collaborative effort, and SSA and IRS are legally bound to the mutually agreed upon purpose and functions.[50] Specifically, the CAWR MOU covers the collaborative processes through which SSA and IRS share earnings information, including establishing clear roles and responsibilities for this effort, as called for by leading practices for inter-agency collaboration.[51]

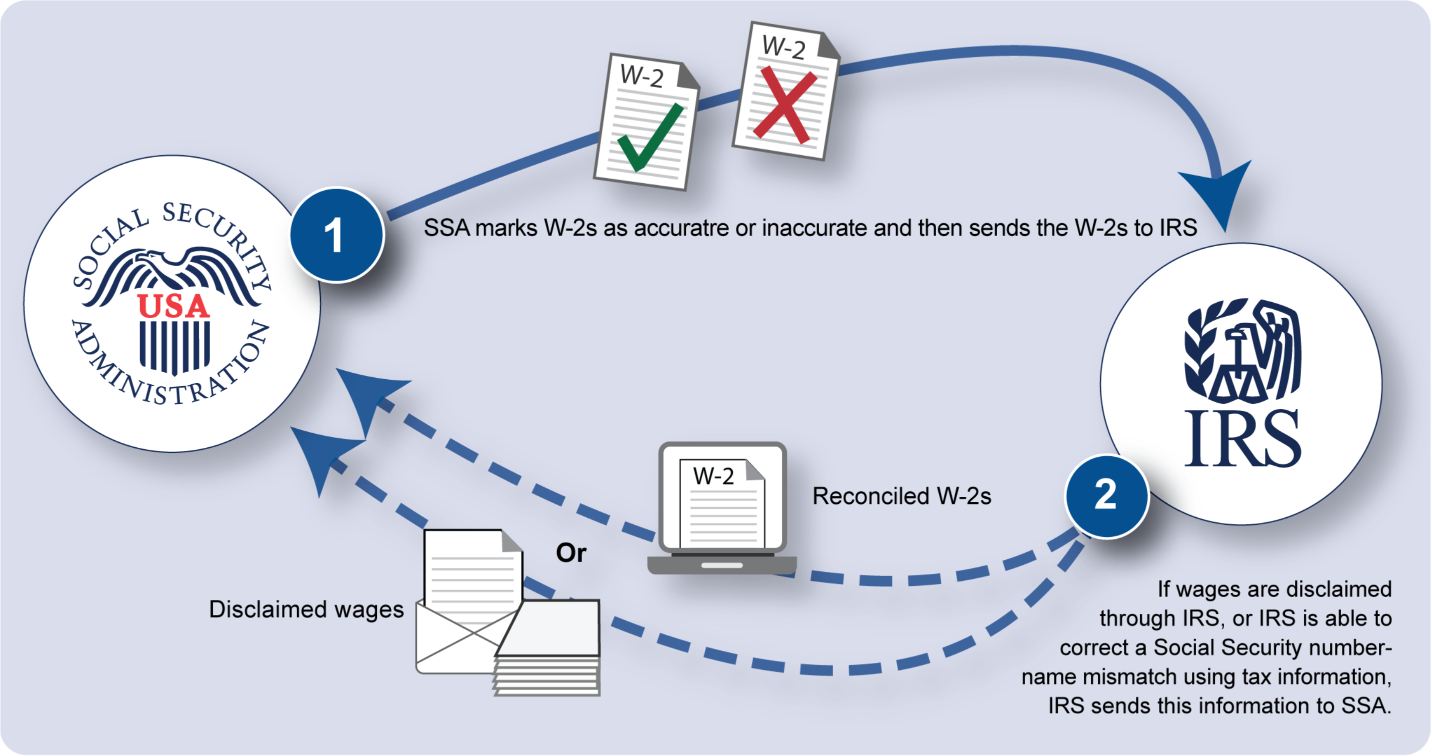
IRS oversees tax administration, including ensuring compliance with tax laws. SSA acts as an agent to these activities by processing W-2s. As illustrated in figure 6, processes covered by the CAWR MOU include SSA sending accurate and inaccurate W-2s to IRS. Also, if wages are disclaimed through IRS, or IRS is able to correct a Social Security number-name mismatch using tax information, IRS sends this information to SSA. Federal law requires the Commissioner of Social Security and the Secretary of the Treasury to share W-2 information, and permits use of the CAWR MOU to effectuate this process.[52] It also requires that the MOU remain in full force and in effect until modified or otherwise changed by mutual agreement of the heads of each agency.

[50] 42 U.S.C. § 432.

[51] GAO-12-1022.

[52] 42 U.S.C. § 432.

Figure 6: Selected Internal Revenue Service (IRS) and Social Security Administration (SSA) Earnings Information Exchanges


W-2
W-2
1
SSA marks W-2s as accuratre or inaccurate and then sends the W-2s to IRS
W-2
Reconciled W-2s
2
Or
Disclaimed wages
If wages are disclaimed through IRS, or IRS is able to correct a Social Security number-name mismatch using tax information, IRS sends this information to SSA.

Source: GAO review of SSA and IRS documents. I GAO-20-492

SSA and IRS Have Been Working to Update the 2007 CAWR MOU Since 2016

SSA and IRS have taken steps to update the 2007 CAWR MOU, but the effort has been underway for more than 3 years. As we reported in September 2012, continually updating agreements is an important part of the leading practice for written guidance and agreements.[53]

SSA and IRS officials told us that discussions about the update began in 2012 and the substantive work of updating the MOU began in August 2016. Since the MOU has not been updated in more than a decade, certain data-exchange materials and provisions in the MOU have become outdated, such as the references to microfilm.

[53] GAO-12-1022.

According to SSA and IRS officials, the MOU update has been driven by efforts at the staff level with executives briefed on the status. We have previously found that leadership involvement in collaborative efforts is needed to overcome the many barriers to working across agency boundaries.[54] SSA officials noted that having highly involved executives would indicate problems with the MOU update process. IRS officials said that the staff level is the appropriate place to negotiate the MOU update with oversight from executives, as needed. However, at both agencies, officials at the staff level do not have the authority to agree to any updates or modifications of the MOU. SSA and IRS are responsible for ensuring the MOU update process is thorough, complete, and carried out in a timely manner.

SSA and IRS officials stated that while the MOU is the cornerstone of SSA-IRS collaboration, completing the update is challenging because there are competing priorities. Additionally, the agencies are not legally required to update the MOU; instead, the MOU is in effect until modified or otherwise changed by mutual agreement of the Commissioner of Social Security and the Secretary of the Treasury (who delegated this authority to the Commissioner of Internal Revenue).

In September 2019, SSA and IRS officials told us they plan to complete the update of the MOU in spring 2020, more than 3-and-a-half years after the effort to update the MOU began. Standards for project management call for developing a plan with specific actions and time frames.[55] A plan could also identify the resources, processes, and individuals necessary to carry out the update. SSA and IRS officials acknowledged that they did not develop such a plan for the ongoing effort to update the MOU. By developing a plan for future updates that includes actions, time frames, and responsible individuals, including executive leadership, SSA and IRS would have greater assurance that the MOU would be updated when needed.

[54] GAO-06-15.

[55] Project Management Institute, Inc. *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)*, Sixth Edition, 2017.

SSA and IRS Have Not Developed Shared Goals and Performance Measures or Conducted Required Annual Reviews of the MOU Process

While SSA and IRS have established joint functions in the CAWR MOU, the agencies do not have shared goals and performance measures to help track progress in implementing these functions and identify potential improvements. As we reported in September 2012, defining short- and long-term outcomes is an important part of the leading practice for outcomes and accountability for collaborative efforts.[56] This includes defining and articulating common goals based on what the group shared in common and developing mechanisms, such as performance goals and measures, to evaluate the results.

SSA officials said existing goals and measures in the MOU were sufficiently effective. However, we did not find evidence of goals and measures in the MOU and neither SSA nor IRS officials could provide documentation of specific examples of such. Establishing shared goals and performance measures for the CAWR MOU functions would help SSA and IRS monitor and evaluate its results, as well as identify potential weaknesses and potential improvements.

While the MOU lacks goals and measures, it does contain provisions for the agencies to conduct annual studies of the CAWR process and to submit a report to each commissioner on the results. However, the agencies have not consistently implemented these provisions. Monitoring progress is an important part of the leading practice for outcomes and accountability for collaborative efforts. Continually monitoring agreements is an important part of the leading practice for written guidance and agreements.[57] For SSA and IRS, this means monitoring progress toward fulfilling their legal obligation to implement the CAWR MOU.[58]

In the 2007 CAWR MOU, SSA and IRS agreed to the following monitoring provisions related to conducting an annual review of the CAWR process.

- **Conduct annual joint studies of the CAWR process.** Since the MOU was implemented in 2007, IRS and SSA have not conducted a

[56] GAO-12-1022.

[57] GAO-12-1022.

[58] 42 U.S.C. § 432.

joint study of the CAWR process. These reviews were intended to assist the required annual review of the MOU and help inform the agencies of potential improvements to the CAWR process. Specifically, the MOU requires that upon completion of the annual review, a joint SSA and IRS report should be sent to each commissioner consisting of the results of the review, a list of any changes that have occurred in the process, and any recommendation for changes. This is intended to serve as an important monitoring function for the MOU. IRS officials said the agencies have been unable to conduct annual joint studies or submit the required annual reports primarily because the MOU is extensive and affects many offices at both agencies. SSA and IRS officials said that they plan to change to a biannual interagency review of the MOU so they can do a better job of keeping the MOU updated and relevant. However, officials did not provide information about any steps they plan to take to ensure that the reviews would occur as required.

According to SSA officials, SSA and IRS plan to meet every 3 or 6 months to review existing agreements, including the CAWR MOU. This may be a means of identifying necessary changes to the CAWR process since regular communication can facilitate effective collaboration; however, officials did not provide additional details on these potential new meetings.

- **Conduct annual independent studies of the CAWR process.** SSA had no records that it had conducted an independent study of the process in the past 3 years. IRS conducted two independent studies in 2018 on the CAWR process which primarily focused on IRS's adherence to its policy guidance. Annual independent studies were intended to serve as another feedback mechanism to assist in the review of the MOU.

According to SSA and IRS officials, they have not implemented these monitoring provisions because of resource constraints. As previously discussed, the agencies are updating the CAWR MOU and plan to finalize the updated MOU by spring 2020. Officials told us that, similar to the 2007 MOU, the updated MOU will include requirements for periodically reviewing the MOU to identify potential improvements to the CAWR process. However, the time frames may change. Developing and documenting a strategy for implementing the monitoring provisions in the updated MOU would provide greater assurance that SSA and IRS are periodically assessing the CAWR process and identifying opportunities for improvement, as required.

SSA and IRS Have Developed Ways to Operate Across Agency Boundaries, but Lack Sufficient Common Terminology Related to the CAWR Process and Identity Fraud

As we reported in September 2012, agreeing on common terminology and definitions is an important part of bridging organizational cultures.[59] One way to operate across agency boundaries is to foster open lines of communication. SSA and IRS do this by holding interagency meetings, including quarterly executive-level and monthly technical-level meetings. In addition, officials from SSA and IRS said that the agencies have a strong working relationship and that officials at both agencies have frequent informal communication. The agencies also established a fraud working group, which held introductory meetings in 2018 and 2019. While the group does not have a formal mission statement, the general scope of responsibility for the group is to identify areas of common interest related to mitigating fraud and to collaborating on best practices and efforts to mitigate fraud risks.

However, SSA and IRS have developed limited common terminology and definitions related to their CAWR collaboration effort. The agencies have agreed on 10 definitions in their MOU, but these definitions are very limited in scope; for example, two of these definitions simply spell out the agency names and none of the definitions are for the 20 data variables the agencies exchange daily.

Both SSA and IRS officials stated that common terminology related to identity fraud would be helpful, and acknowledged that they use different terminology and have to call each other to ask what different terms mean. SSA officials cited the use of different terminology at SSA and IRS as a barrier to collaboration.

Because of the absence of common terminology, IRS has been unaware of information it receives from SSA in some cases. For example, through the common format record exchange, SSA shares information with IRS about why SSA determined that a W-2 is inaccurate, but IRS was unaware of this information. SSA told us that it sends a table to IRS

[59] GAO-12-1022.

annually that includes code combinations for their data transfers and their meanings which explain why the W-2 was accurate or inaccurate.

However, SSA officials were unsure of the extent to which IRS officials understood the codes. One reason that SSA determines a W-2 is inaccurate is if earnings with the same name, SSN, and EIN were disclaimed in previous years. SSA communicates this to IRS using codes within the W-2 record that are labeled "invalid due to SWED."[60] However, SSA and IRS have not defined "SWED" and IRS officials said that they were unaware of receiving information from SSA about previously disclaimed wages. Officials said they interpreted the information to relate to invalid wages due to name and SSN mismatches and spent time trying to resolve the mismatch issue. They said that such information could be useful for future enforcement efforts. Further, IRS officials said that they were also unaware of other code combinations that SSA officials told us they use to inform IRS about accurate and inaccurate wages.

IRS attributed its unfamiliarity with the data elements coming from SSA to staff turnover since key IRS officials who were familiar with the data elements retired. However, IRS could have been aware of the meaning of the variables if the agencies had established and documented common definitions for these data elements. In addition, according to IRS officials, they have limited resources for following up on information that SSA is sharing because they have been focused on competing priorities, including implementing the Tax Cuts and Jobs Act of 2017.

SSA and IRS officials noted that the next version of the MOU will define additional terminology that was not defined in previous MOU documents. For example, officials said that "EIN" and "TIN" are key IRS terminology that may be defined in the new MOU.[61] Until SSA and IRS clearly define the data elements they exchange as part of the CAWR process, SSA and IRS are at risk of not communicating effectively about CAWR and, thus, missing opportunities to use data more effectively to identify fraudulent or otherwise inaccurate W-2s. This could be done, for example, by

[60] SSA assigns a special indicator—Scrambled Wage Earnings Discrepancy (SWED)—when number holders disclaim the wages.

[61] An employer identification number (EIN) is a nine-digit number assigned by IRS. It is used to identify the tax accounts of employers and certain others who have no employees. IRS uses the number to identify taxpayers who are required to file various business tax returns. A Taxpayer Identification Number (TIN) is an identification number used by IRS in the administration of tax laws. It is issued either by SSA or IRS. A SSN is issued by the SSA whereas all other TINs are issued by IRS.

developing a shared data dictionary that clearly defines all of the data elements the agencies are exchanging.

Conclusions

Employment-related identity fraud can have negative impacts on victims and poses risks to both SSA and IRS. Victims may face IRS enforcement actions or a reduction in benefits for some federal programs based on wages earned by fraudsters. The full scope of this fraud is unknown. In 2018, IRS marked more than 800,000 taxpayer accounts with Action Code 525 “employment-related identity theft.” However, IRS’s use of the term “employment-related identity theft” likely understates the true scope and impact of this type of fraud and may be misleading to both agency decision makers and Congress. Additionally, by assessing the feasibility of incorporating additional compliance checks into its checks of employment-related identity fraud, IRS may be able to develop a method for identifying additional taxpayers at risk of this type of fraud.

SSA and IRS rely on accurate W-2 information to carry out their missions and have taken steps to detect the submission of fraudulent W-2s. Evaluating the costs and benefits of expanding IRS’s Withholding Compliance Program (WHC) to include cases with mismatched names and SSNs may provide IRS an opportunity to increase revenue collection.

Additionally, while IRS has taken steps to manage the impacts of identity fraud on victims, the agency’s decision to exclude approximately 3 million individuals with IDT action codes from Automated Underreporter’s (AUR) wage discrepancy checks has resulted in a gap in enforcement coverage. IRS plans to update most of the agency’s legacy programming code by the end of fiscal year 2024. Updating AUR’s programming to include these individuals would enable IRS to close this enforcement gap and potentially increase revenue.

Further, SSA and IRS’s 2007 CAWR MOU plays an important role in IRS and SSA’s efforts to accurately report wage information and resolve mismatches. While the agencies expect to finalize their first update of the MOU by spring 2020, efforts to update the MOU have been ongoing for more than 3 years. Developing a plan for implementing future updates would provide greater assurance that the MOU would be updated when needed. Additionally, developing performance goals and measures for the MOU as well as a strategy for assuring the studies called for by the MOU are completed within the specified time frames would help ensure that

SSA and IRS are periodically assessing the CAWR process, and identifying opportunities for improvement. Moreover, by clearly defining the data elements IRS and SSA exchange as part of the CAWR process, the agencies would be better positioned to effectively use the data to identify fraudulent or otherwise inaccurate W-2s.

Recommendations for Executive Action

We are making a total of 12 recommendations, including eight to IRS and four to SSA.

The Commissioner of Internal Revenue should modify the title of IRS's employment-related identity theft action code 525 to reflect the type of employment-related identity fraud encompassed by this action code. (Recommendation 1)

The Commissioner of Internal Revenue should assess and document the feasibility of incorporating additional checks into its automated checks of employment-related identity fraud for populations at risk of employment-related identity fraud, such as children, elderly, deceased persons, and individuals associated with multiple wage records. (Recommendation 2)

The Commissioner of Internal Revenue should assess and document the costs and benefits of using WHC to address compliance risks posed by potential employment-related identity fraudsters who owe taxes and take appropriate action, as needed. (Recommendation 3)

The Commissioner of Internal Revenue should modify AUR to include wage discrepancy checks for victims of employment-related identity fraud once IRS has updated AUR's legacy programming code. (Recommendation 4)

The Commissioner of Internal Revenue should, in collaboration with the Commissioner of Social Security, develop and document a plan for updating future CAWR MOUs. The plan should identify actions, time frames, and responsible parties, including executive leadership. (Recommendation 5)

The Commissioner of Internal Revenue should, in collaboration with the Commissioner of Social Security, develop and implement goals and performance measures for the CAWR MOU. (Recommendation 6)

The Commissioner of Internal Revenue should, in collaboration with the Commissioner of Social Security, develop and document a strategy for assuring that the reviews required by the updated MOU are completed within the specified time frames. (Recommendation 7)

The Commissioner of Internal Revenue should, in collaboration with the Commissioner of Social Security, clearly define data elements they exchange with SSA. (Recommendation 8)

The Commissioner of Social Security should, in collaboration with the Commissioner of Internal Revenue, develop and document a plan for updating future CAWR MOUs. The plan should identify actions, time frames, and responsible parties, including executive leadership. (Recommendation 9)

The Commissioner of Social Security should, in collaboration with the Commissioner of Internal Revenue, develop and implement goals and performance measures for the CAWR MOU. (Recommendation 10)

The Commissioner of Social Security should, in collaboration with the Commissioner of Internal Revenue, develop and document a strategy for assuring that the reviews required by the updated MOU are completed within the specified time frames. (Recommendation 11)

The Commissioner of Social Security should, in collaboration with the Commissioner of Internal Revenue, clearly define the data elements they exchange with IRS. (Recommendation 12)

Agency Comments

We provided a draft of the sensitive version of this report to IRS, SSA, the Federal Trade Commission, the Department of Health and Human Services, and the Department of Homeland Security for comment. In comments reproduced in appendix II, IRS neither agreed nor disagreed with the recommendations. In comments reproduced in appendix III, SSA agreed with the recommendations and noted that SSA and IRS officials are meeting on a recurring basis to complete an updated memorandum of understanding. IRS, SSA, the Department of Homeland Security, and the Federal Trade Commission provided technical comments which were incorporated as appropriate. The Department of Health and Human Services had no comments on the report.

We are sending copies of this report to the appropriate congressional committees, the Commissioner of Internal Revenue, Commissioner of Social Security, Chairman of the Federal Trade Commission, Secretary of Health and Human Services, Acting Secretary of Homeland Security, Secretary of the Treasury, and other interested parties. In addition, the report is available at no charge on the GAO website at https://www.gao.gov

If you or your staff have any questions about this report, please contact Jessica Lucas-Judy at (202) 512-9110 or LucasJudyJ@gao.gov, or Rebecca Shea at (202) 512-6722 or SheaR@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs are on the last page of this report. GAO staff who made key contributions to this report are listed in appendix IV.

Jessica Lucas-Judy
Director, Tax Issues
Strategic Issues

Rebecca Shea

Rebecca Shea
Director
Forensic Audits and Investigative Service

Appendix I: Objectives, Scope, and Methodology

This report examines (1) the potential scope of employment-related identity fraud, including what the Internal Revenue Service (IRS) knows about this type of fraud and what we could determine by analyzing the Department of Health and Human Services' National Directory of New Hires (NDNH) and IRS data; (2) Social Security Administration (SSA) actions to detect and deter this fraud as well as notify victims; (3) IRS actions to detect and deter this fraud as well as notify victims; and (4) the extent to which SSA and IRS are collaborating to address the issue.

To describe and analyze the potential scope of employment-related identity fraud, we took the following steps:

1. **Identified groups at risk of identity theft.** We first reviewed Treasury Inspector General for Tax Administration, SSA Office of the Inspector General, and our prior reports on Social Security number (SSN) misuse to determine common characteristics of individuals who are at risk of SSN misuse.[1] These characteristics include being deceased, elderly, a child, or having three or more wage records during the 3-month period of our review. Based on these reports, we defined "elderly" as over age 84 and "children" as under age 14 for the purposes of this review.
2. **Identified SSNs at risk of SSN misuse.** We used SSA's full death file for dates of death for deceased individuals, and its Numerical Index File (Numident) for dates of birth for living individuals.[2] We next compared full death file and Numident data to a quarterly extract of NDNH data listing the names and SSNs of individuals who earned wages between August and October 2016. We selected data from this quarter because, at the time of our review, these were the oldest data for which relevant IRS tax data were also available. We used this

[1] GAO, *Supplemental Security Income: Wages Reported for Recipients Show Indications of Possible SSN Misuse*, GAO-14-597 (Washington, D.C.: July 16, 2014), Treasury Inspector General for Tax Administration, *Efforts Are Resulting in the Improved Identification of Fraudulent Tax Returns Involving Identity Theft*, 2015-40-026 (Washington, D.C.: Apr. 24, 2015), and SSA Office of the Inspector General, *Improper Use of Elderly Individuals' Social Security Numbers*, A-03-16-24028 (Baltimore, MD: Jan. 3, 2017).

comparison to identify individuals employed between August and October 2016 who also met at least one of these at-risk characteristics.

NDNH is a database of individuals employed in the United States. Data are collected and reported by state workforce agencies and federal agencies, and the database is administered by the Department of Health and Human Services' Office of Child Support Enforcement. NDNH data are comprised of three types: verified, unverified, and unverifiable. The verified data—used in this analysis—have been checked against SSA records to confirm that the name and SSN match SSA records. Unverified data include data that do not match on name or SSN, and unverifiable data include data that did not include enough information to attempt a match (e.g., when states submit partial or missing name information).

According to the Department of Health and Human Services, there were 584,013,484 verified wage records, 18,629,720 unverified, and 91,134,352 unverifiable as of December 31, 2018. Verified data were used in this analysis to make the estimate more conservative since cases of potential synthetic identity theft—where the name and SSN do not match—are excluded from verified data.

NDNH is designed to assist state child support agencies in locating parents and taking appropriate, interstate actions concerning child support orders. Some authorized agencies also use NDNH data to help prevent overpayments and detect fraud. For example, IRS has access to NDNH to administer the Earned Income Tax Credit. However, IRS and SSA are not authorized to use NDNH information to detect potential employment-related identity fraud.[2]

3. **Identified at-risk individuals with possible tax compliance issues.** We used data from IRS's Compliance Data Warehouse (CDW), a database of taxpayer data, to analyze the wage reporting characteristics of individuals within the NDNH extract we identified as at risk of identity fraud. We categorized taxpayers as potential victims of employment-related identity fraud with possible compliance issues if (1) our analysis of NDNH data showed characteristics associated with being deceased, elderly, a child, or earning wages from three or

[2] We were authorized to use NDNH through the GAO Access and Oversight Act of 2017, Pub. L. No. 115-3, 131 Stat. 7.

more employers in 2016; and (2) at least one employer-submitted Form W-2, Wage and Tax Statement (W-2) was not reported on a 2016 tax return.[3]

When possible, we also limited the analysis to cases where the taxpayer had a known filing requirement.[4] We also identified cases that were consistent with misuse of SSNs for employment-related identity fraud, rather than taxpayer noncompliance. However, we were unable to determine the total extent of taxpayer noncompliance for taxpayers included in this analysis.

Our analysis is not intended to be a comprehensive effort to identify all potential cases of employment-related identity fraud. We focused our analysis on cases where matching names and SSNs were used to obtain employment. These cases pose a risk to SSA, IRS, and victims, yet little is known about these cases.

4. **Analyzed tax characteristics of potential employment-related identity theft victims and other taxpayers.** Last, we used CDW to analyze selected tax characteristics of both individuals we identified as having at least one employer-submitted Form W-2 that was not reported on a 2016 tax return as well as those where employer-submitted Forms W-2 were reported. For example, we analyzed data on wage withholding rates, the prevalence of selected IRS identity theft indicators on taxpayers' accounts, and IRS enforcement actions taken against these individuals.

We assessed IRS procedures against the information gathering and data analytics leading practices in the *Framework for Managing Fraud Risks in Federal Programs.*[5] We did not conduct a comprehensive fraud risk assessment of the IRS enforcement programs. Our assessment was

[3] We clarify that all individuals we identified as having indicators of identity fraud are "potential" victims because, for example, some of these individuals may have actually earned the employer-reported wages but either intentionally or unintentionally failed to include them on a tax return.

[4] Filing requirements differ for each taxpayer. As result, we took a conservative approach and compared populations to the highest potential minimum filing requirement for 2016. For the deceased, the elderly, and individuals with three or more wage records, we used the IRS earned income threshold for married filing jointly where both spouses over age 65, which is $23,300. For children, the earned income threshold was $7,850.

[5] GAO, *A Framework for Managing Fraud Risks in Federal Programs*, GAO-15-593SP (Washington, D.C.: July 2015).

limited to the control activities surrounding employment-related identity fraud.[6]

We assessed the reliability of the full death file, Numident, NDNH quarterly wage data, and selected elements of CDW by reviewing relevant documentation, interviewing knowledgeable agency officials, and performing electronic testing to determine the validity of specific data elements in the data. We determined that the data elements used in our analysis were sufficiently reliable for the purpose of our work to describe and analyze the potential scope of employment-related identity fraud.

To assess IRS and SSA actions to detect and prevent employment-related identity fraud as well as notify victims, we reviewed relevant documentation including IRS's *Internal Revenue Manual* and SSA's *Policy Operations Manual System*. We also interviewed knowledgeable officials from both agencies on SSA and IRS processes for detecting and preventing employment-related identity fraud and notifying victims. We compared IRS's and SSA's efforts to relevant federal internal control standards.[7] We also assessed the agencies' efforts against IRS and SSA's respective strategic plans as well as select leading practices to combat fraud, as identified in the *Framework for Managing Fraud Risks in Federal Programs.*[8]

To evaluate the extent to which IRS and SSA are effectively collaborating to address employment-related identity fraud, we reviewed relevant agency documents, such as IRS and SSA's Combined Annual Wage Reporting Memorandum of Understanding, other IRS-SSA legal agreements, meeting minutes from IRS-SSA joint meetings, and policy manuals. Because of its role with assisting victims and collecting statistics on identity theft, we interviewed agency officials from the Federal Trade Commission in addition to knowledgeable officials from IRS and SSA. Because of its role helping employers verify the identities of employees, we interviewed officials at the Department of Homeland Security.

We focused our assessment on SSA and IRS because those agencies are most directly involved in the wage reporting process used to detect

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

[7] GAO-14-704G.

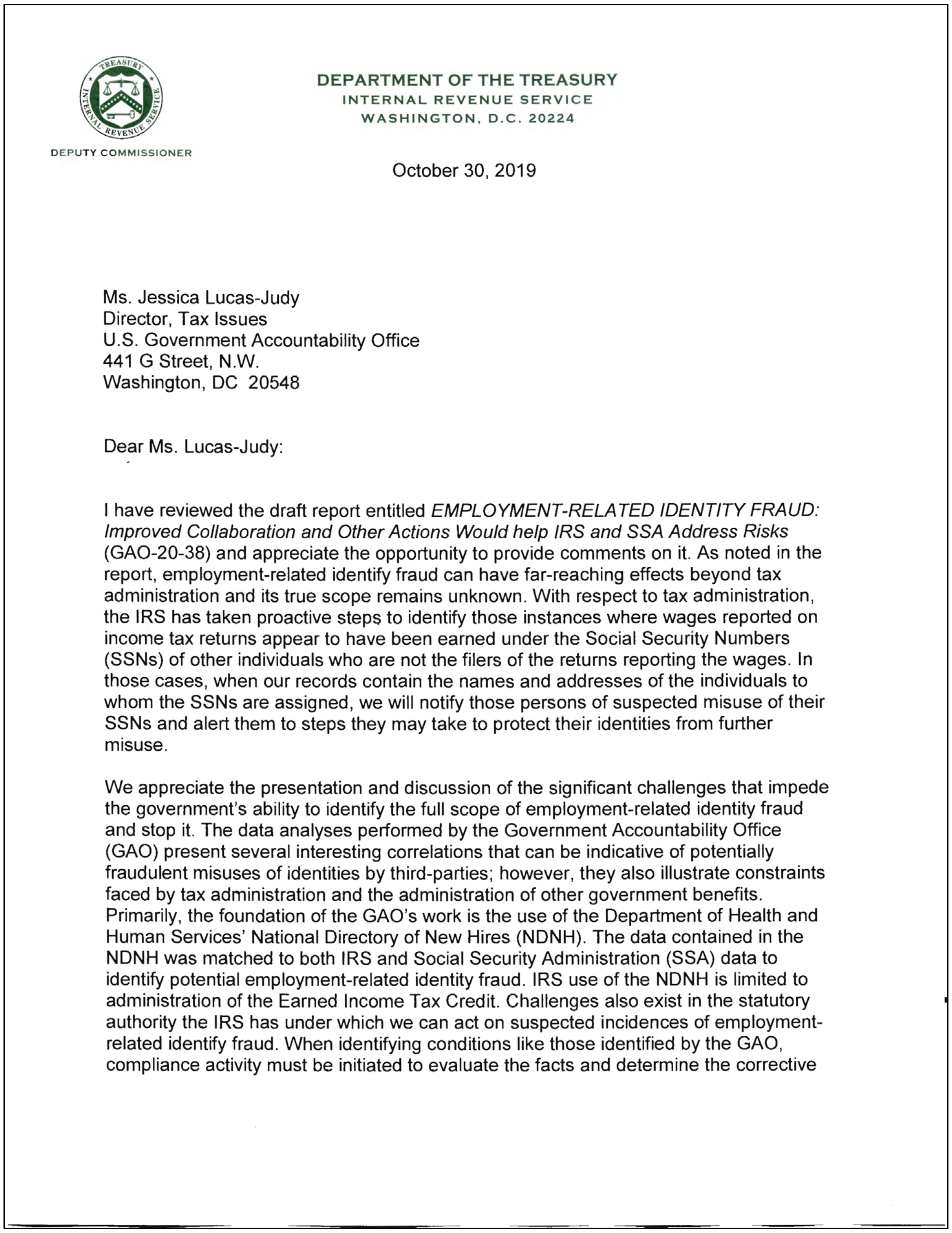
[8] GAO-15-593SP.

and resolve employment-related identity fraud. We assessed IRS and SSA's collaboration efforts against leading practices for collaboration we have identified in our prior work and against standards for project management.[9] We identified key elements of each leading practice and assessed the extent to which SSA and IRS collaboration on employment-related identity theft aligned with leading practices or key elements.

The performance audit upon which this report is based was conducted from November 2017 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. We worked with SSA from October 2019 to May 2020 to prepare this public version of the original sensitive report for public release. This public version was also prepared in accordance with these standards.

[9] GAO, *Managing for Results: Key Considerations for Implementing Interagency Collaborative Mechanisms*, GAO-12-1022 (Washington D.C.: Sept. 27, 2012), *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, GAO-06-15 (Washington, D.C.: Oct. 21, 2005), and Project Management Institute, Inc. *A Guide to the Project Management Body of Knowledge (PMBOK® Guide), Sixth Edition*, 2017.

Appendix II: Comments from the Internal Revenue Service



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

DEPUTY COMMISSIONER

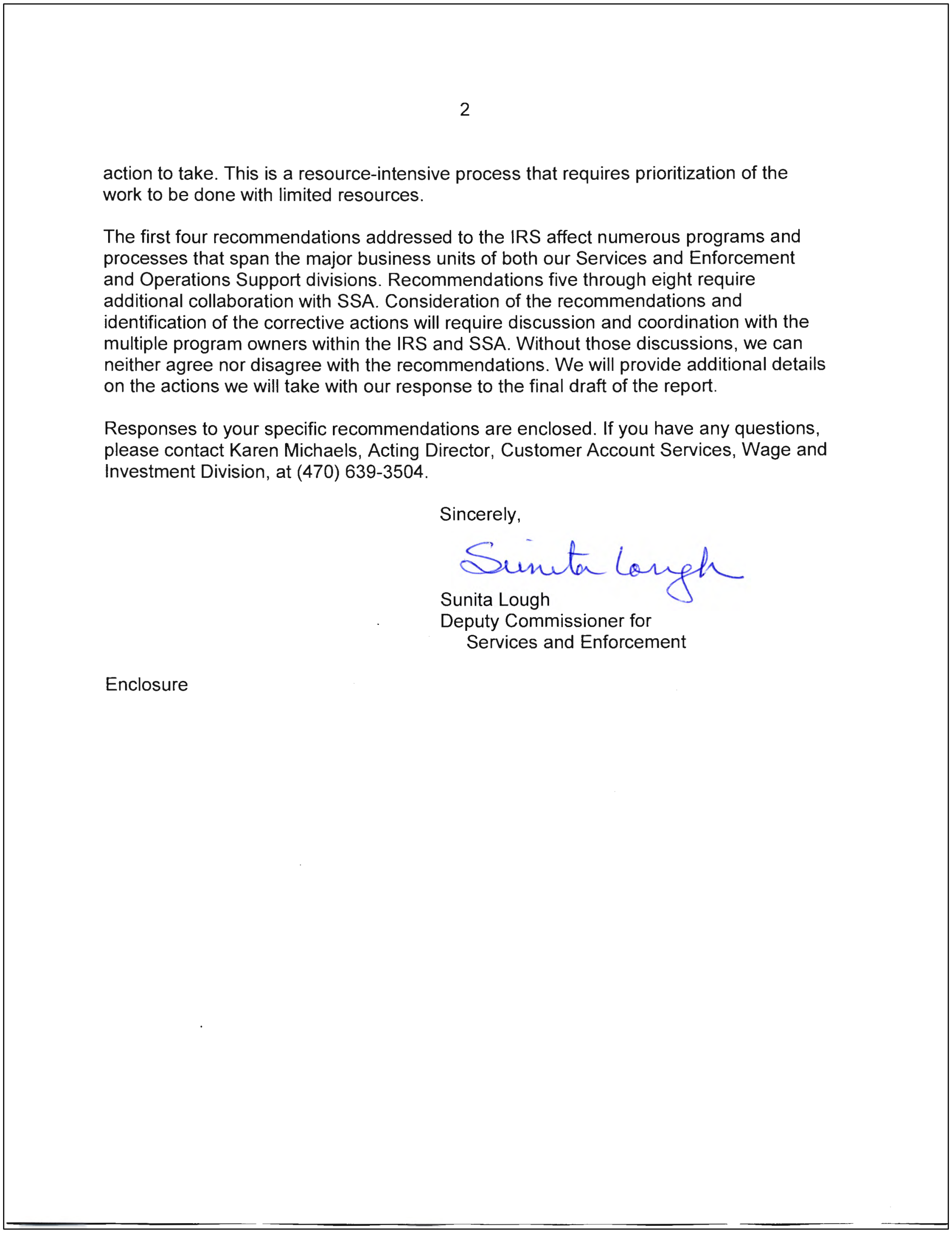
October 30, 2019

Ms. Jessica Lucas-Judy
Director, Tax Issues
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Ms. Lucas-Judy:

I have reviewed the draft report entitled *EMPLOYMENT-RELATED IDENTITY FRAUD: Improved Collaboration and Other Actions Would help IRS and SSA Address Risks* (GAO-20-38) and appreciate the opportunity to provide comments on it. As noted in the report, employment-related identify fraud can have far-reaching effects beyond tax administration and its true scope remains unknown. With respect to tax administration, the IRS has taken proactive steps to identify those instances where wages reported on income tax returns appear to have been earned under the Social Security Numbers (SSNs) of other individuals who are not the filers of the returns reporting the wages. In those cases, when our records contain the names and addresses of the individuals to whom the SSNs are assigned, we will notify those persons of suspected misuse of their SSNs and alert them to steps they may take to protect their identities from further misuse.

We appreciate the presentation and discussion of the significant challenges that impede the government's ability to identify the full scope of employment-related identity fraud and stop it. The data analyses performed by the Government Accountability Office (GAO) present several interesting correlations that can be indicative of potentially fraudulent misuses of identities by third-parties; however, they also illustrate constraints faced by tax administration and the administration of other government benefits. Primarily, the foundation of the GAO's work is the use of the Department of Health and Human Services' National Directory of New Hires (NDNH). The data contained in the NDNH was matched to both IRS and Social Security Administration (SSA) data to identify potential employment-related identity fraud. IRS use of the NDNH is limited to administration of the Earned Income Tax Credit. Challenges also exist in the statutory authority the IRS has under which we can act on suspected incidences of employment-related identify fraud. When identifying conditions like those identified by the GAO, compliance activity must be initiated to evaluate the facts and determine the corrective



action to take. This is a resource-intensive process that requires prioritization of the work to be done with limited resources.

The first four recommendations addressed to the IRS affect numerous programs and processes that span the major business units of both our Services and Enforcement and Operations Support divisions. Recommendations five through eight require additional collaboration with SSA. Consideration of the recommendations and identification of the corrective actions will require discussion and coordination with the multiple program owners within the IRS and SSA. Without those discussions, we can neither agree nor disagree with the recommendations. We will provide additional details on the actions we will take with our response to the final draft of the report.

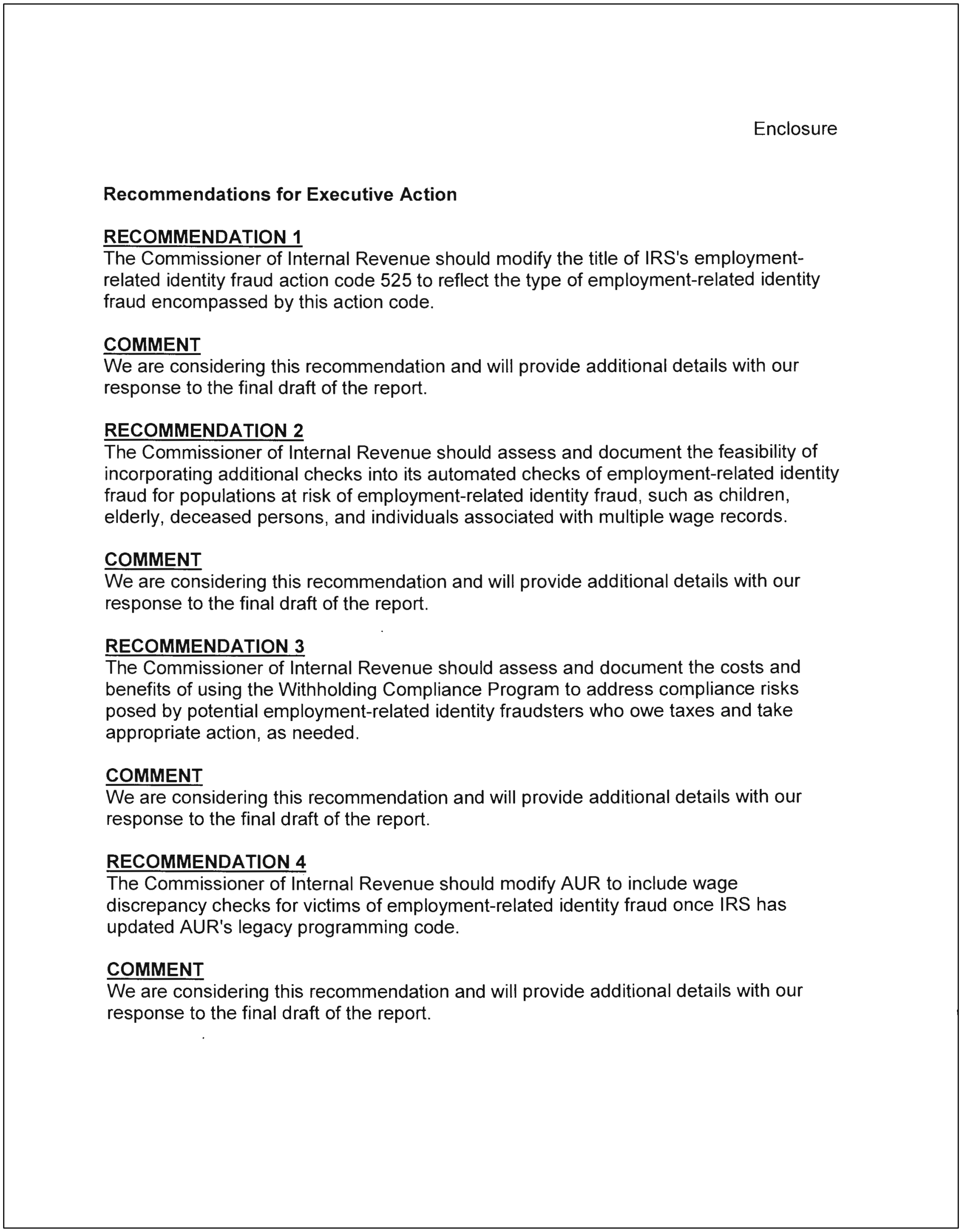
Responses to your specific recommendations are enclosed. If you have any questions, please contact Karen Michaels, Acting Director, Customer Account Services, Wage and Investment Division, at (470) 639-3504.

Sincerely,

Sunita Lough

Sunita Lough
Deputy Commissioner for
Services and Enforcement

Enclosure



Enclosure

Recommendations for Executive Action

RECOMMENDATION 1
The Commissioner of Internal Revenue should modify the title of IRS's employment-related identity fraud action code 525 to reflect the type of employment-related identity fraud encompassed by this action code.

COMMENT
We are considering this recommendation and will provide additional details with our response to the final draft of the report.

RECOMMENDATION 2
The Commissioner of Internal Revenue should assess and document the feasibility of incorporating additional checks into its automated checks of employment-related identity fraud for populations at risk of employment-related identity fraud, such as children, elderly, deceased persons, and individuals associated with multiple wage records.

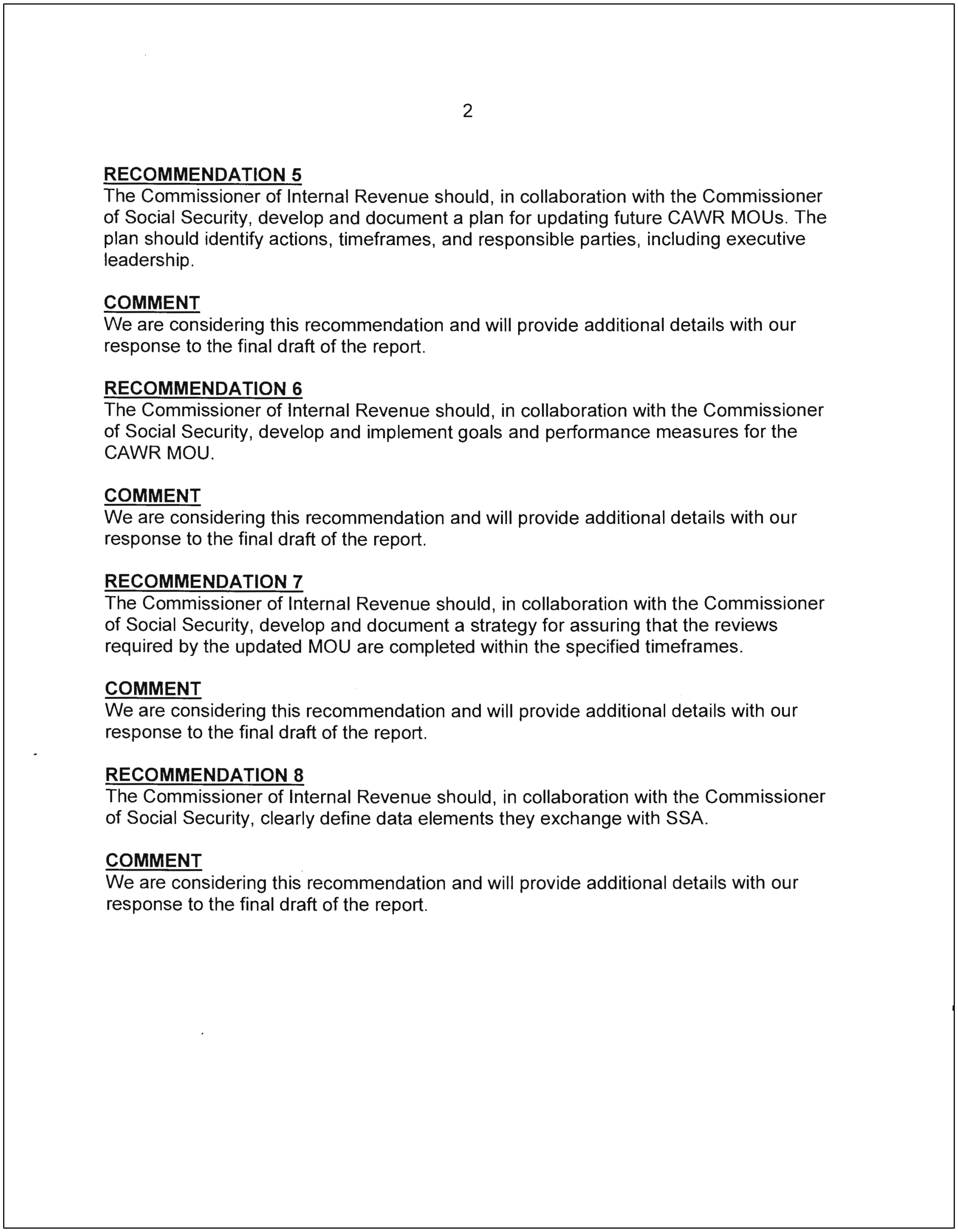
COMMENT
We are considering this recommendation and will provide additional details with our response to the final draft of the report.

RECOMMENDATION 3
The Commissioner of Internal Revenue should assess and document the costs and benefits of using the Withholding Compliance Program to address compliance risks posed by potential employment-related identity fraudsters who owe taxes and take appropriate action, as needed.

COMMENT
We are considering this recommendation and will provide additional details with our response to the final draft of the report.

RECOMMENDATION 4
The Commissioner of Internal Revenue should modify AUR to include wage discrepancy checks for victims of employment-related identity fraud once IRS has updated AUR's legacy programming code.

COMMENT
We are considering this recommendation and will provide additional details with our response to the final draft of the report.



RECOMMENDATION 5
The Commissioner of Internal Revenue should, in collaboration with the Commissioner of Social Security, develop and document a plan for updating future CAWR MOUs. The plan should identify actions, timeframes, and responsible parties, including executive leadership.

COMMENT
We are considering this recommendation and will provide additional details with our response to the final draft of the report.

RECOMMENDATION 6
The Commissioner of Internal Revenue should, in collaboration with the Commissioner of Social Security, develop and implement goals and performance measures for the CAWR MOU.

COMMENT
We are considering this recommendation and will provide additional details with our response to the final draft of the report.

RECOMMENDATION 7
The Commissioner of Internal Revenue should, in collaboration with the Commissioner of Social Security, develop and document a strategy for assuring that the reviews required by the updated MOU are completed within the specified timeframes.

COMMENT
We are considering this recommendation and will provide additional details with our response to the final draft of the report.

RECOMMENDATION 8
The Commissioner of Internal Revenue should, in collaboration with the Commissioner of Social Security, clearly define data elements they exchange with SSA.

COMMENT
We are considering this recommendation and will provide additional details with our response to the final draft of the report.

Text of Appendix II: Comments from the Internal Revenue Service

Page 1

Department of the Treasury
Internal Revenue Service
Washington, D.C. 20224

Ms. Jessica Lucas-Judy

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

Dear Ms. Lucas-Judy:

I have reviewed the draft report entitled EMPLOYMENT-RELATED IDENTITY FRAUD: Improved Collaboration and Other Actions Would help IRS and SSA Address Risks (GAO-20-38) and appreciate the opportunity to provide comments on it. As noted in the report, employment-related identify fraud can have far-reaching effects beyond tax administration and its true scope remains unknown. With respect to tax administration, the IRS has taken proactive steps to identify those instances where wages reported on income tax returns appear to have been earned under the Social Security Numbers (SSNs) of other individuals who are not the filers of the returns reporting the wages. In those cases, when our records contain the names and addresses of the individuals to whom the SSNs are assigned, we will notify those persons of suspected misused of their SSNs and alert them to steps they may take to protect their identities from further misuse.

We appreciate the presentation and discussion of the significant challenges that impedes the government's ability to identify the full scope of employment-related identity fraud and stop it. The data analyses performed by the Government Accountability Office (GAO) presents several interesting correlations that can be indicative of potentially fraudulent misuses of identities by third-parties; however, they also illustrate constraints faced by tax administration and the administration of other government benefits. Primarily, the foundation of the GAO's work is the use of the Department of Health and Human Services' National Directory of New Hires (NDNH). The data contained in the NDNH was matched to both IRS and Social Security Administration (SSA) data to identify potential employment-related identity fraud. IRS use of the NDNH is limited to administration of the Earned Income Tax Credit. Challenges also exist in the statutory authority the IRS has under which we can act on suspected incidences of employment-related identify fraud. When identifying conditions like those identified by the GAO, compliance activity must be initiated to evaluate the facts and determine the corrective

Page 2

Action to take. This is a resource-intensive process that requires prioritization of the work to be done with limited resources.

The first four recommendations addressed to the IRS affect numerous programs and processes that span the major business units of both our Services and Enforcement and Operations Support divisions. Recommendation five through eight require additional collaboration with SSA. Consideration of the recommendations and identification for the corrective actions will require discussion and coordination with the multiple program owners within the IRS and SSA. Without those discussions, we can neither agree nor disagree with the recommendations. We will provide additional details on the actions we will take with our response to the final draft of the report.

Responses to your specific recommendations are enclosed. If you have any questions, please contact Karen Michaels, Acting Director, Customer Account Services, Wage and Investment Division, at (470) 639-3504.

Sincerely,

Sunita Lough
Deputy Commissioner for Services and Enforcement

Enclosure

Page 3

Recommendations for Executive Action

RECOMMENDATION 1

The Commissioner of Internal Revenue should modify the title of IRS's employment-related identity fraud action code 525 to reflect the type of employment-related identity fraud encompassed by this action code.

COMMENT

We are considering this recommendation and will provide additional details with our response to the final draft of the report.

RECOMMENDATION 2

The commissioner of Internal Revenue should assess and document the feasibility of incorporating additional checks into its automated checks of employment-related identity fraud for populations at risk of employment-related identity fraud, such as children, elderly deceased persons, and individuals associated with multiple wage records.

COMMENT

We are considering this recommendation and will provide additional details with our response to the final draft of the report.

RECOMMENDATION 3

The Commissioner of Internal Revenue should assess and document the costs and benefits of using the Withholding Compliance Program to address compliance risks posed by potential employment-related identity fraudsters who owe taxes and take appropriate action, as needed.

COMMENT

We are considering this recommendation and will provide additional details with our response to the final draft of the report.

RECOMMENDATION 4

The Commissioner of Internal Revenue should modify AUR to include wage discrepancy checks for victims of employment-related identity fraud once IRS has update AUR’s legacy programming code.

COMMENT

We are considering this recommendation and will provide additional details with our response to the final draft of the report.

<ins>Page 4</ins>

RECOMMENDATION 5

The Commissioner of Internal Revenue should, in collaboration with the Commissioner of Social Security, develop and document a plan for updating future

CAWR MOUs. The plan should identify actions, timeframes, and responsible parties, including executive leadership.

COMMENT

We are considering this recommendation and will provide additional details with our response to the final draft of the report.

RECOMMENDATION 6

The Commissioner of Internal Revenue should, in collaboration with the Commissioner of Social Security, develop and implement goals and performance measures for the CAWR MOU.

COMMENT

We are considering this recommendation and will provide additional details with our response to the final draft of the report.

RECOMMENDATION 7

The Commissioner of Internal Revenue should, in collaboration with the Commissioner of Social Security, develop and document a strategy for assuring that the reviews required by the updated MOU are completed within the specified timeframes.

COMMENT

We are considering this recommendation and will provide additional details with our response to the final draft of the report.

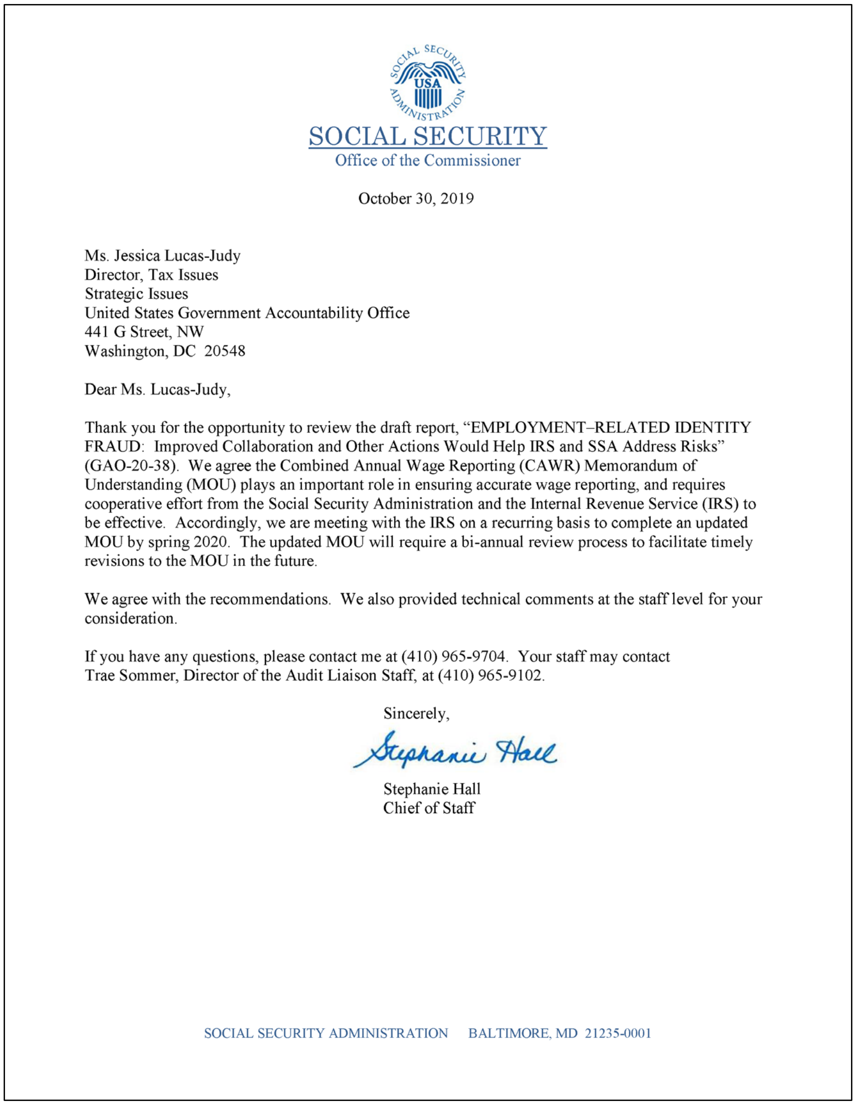
RECOMMENDATION 8

The Commissioner of Internal Revenue should, in collaboration with the Commissioner of Social Security, clearly define data element they exchange with SSA.

COMMENT

We are considering this recommendation and will provide additional details with our response to the final draft of the report.

Appendix III: Comments from the Social Security Administration



SOCIAL SECURITY
Office of the Commissioner

October 30, 2019

Ms. Jessica Lucas-Judy
Director, Tax Issues
Strategic Issues
United States Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Lucas-Judy,

Thank you for the opportunity to review the draft report, "EMPLOYMENT–RELATED IDENTITY FRAUD: Improved Collaboration and Other Actions Would Help IRS and SSA Address Risks" (GAO-20-38). We agree the Combined Annual Wage Reporting (CAWR) Memorandum of Understanding (MOU) plays an important role in ensuring accurate wage reporting, and requires cooperative effort from the Social Security Administration and the Internal Revenue Service (IRS) to be effective. Accordingly, we are meeting with the IRS on a recurring basis to complete an updated MOU by spring 2020. The updated MOU will require a bi-annual review process to facilitate timely revisions to the MOU in the future.

We agree with the recommendations. We also provided technical comments at the staff level for your consideration.

If you have any questions, please contact me at (410) 965-9704. Your staff may contact Trae Sommer, Director of the Audit Liaison Staff, at (410) 965-9102.

Sincerely,

Stephanie Hall

Stephanie Hall
Chief of Staff

SOCIAL SECURITY ADMINISTRATION BALTIMORE, MD 21235-0001

Text of Appendix III: Comments from the Social Security Administration

Page 1

SOCIAL SECURITY
Office of the Commissioner

October 30, 2019

Ms. Jessica Lucas-Judy Director,
Tax Issues Strategic Issues
United States Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Lucas-Judy,

Thank you for the opportunity to review the draft report, "EMPLOYMENT–RELATED IDENTITY FRAUD: Improved Collaboration and Other Actions Would Help IRS and SSA Address Risks" (GAO-20-38). We agree the Combined Annual Wage Reporting (CAWR) Memorandum of Understanding (MOU) plays an important role in ensuring accurate wage reporting, and requires cooperative effort from the Social Security Administration and the Internal Revenue Service (IRS) to be effective. Accordingly, we are meeting with the IRS on a recurring basis to complete an updated MOU by spring 2020. The updated MOU will require a bi-annual review process to facilitate timely revisions to the MOU in the future.

We agree with the recommendations. We also provided technical comments at the staff level for your consideration.

If you have any questions, please contact me at (410) 965-9704. Your staff may contact Trae Sommer, Director of the Audit Liaison Staff, at (410) 965-9102.

Sincerely,

Stephanie Hall
Chief of Staff

SOCIAL SECURITY ADMINISTRATION
BALTIMORE, MD 21235-0001

GAO Contacts

Appendix IV: GAO Contact and Staff Acknowledgments

Jessica Lucas-Judy, (202) 512-9110, LucasJudyJ@gao.gov

Rebecca Shea, (202) 512-6722 or SheaR@gao.gov

Staff Acknowledgments

In addition to the individual named above, the following staff made key contributions to this report: Neil A. Pinney (Assistant Director), Philip D. Reiff (Assistant Director), Melissa L. King (Analyst-in-Charge), Priyanka Sethi Bansal, Heather A. Collins, Ann L. Czapiewski, Celina F. Davidson, Pamela R. Davidson, Julia C. DiPonio, Shannon J. Finnegan, Steven Flint, Robert L. Gebhart, James A. Howard, Grace H. Kwon, Krista Loose, Maria C. McMullen, Kevin C. Metcalfe, J. Daniel Paulk, Lindsay W. Swenson, Sonya Vartivarian, Ariel Vega, and Miranda J. Wickham.

(104107)

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