United States Government Accountability Office

Testimony

Before the Subcommittee on Oversight, Committee on Ways and Means, House of Representatives

For Release on Delivery
Expected at 10 a.m. ET
Tuesday, April 19, 2016

TAX FILING

IRS Needs a Comprehensive Customer Service Strategy and Needs to Better Combat Identity Theft Refund Fraud and Protect Taxpayer Data

Statement of Jessica K. Lucas-Judy, Acting Director, Strategic Issues

GAO-16-578T

GAO Highlights

Highlights of GAO-16-578T, a testimony before the Subcommittee on Oversight, Committee on Ways and Means, House of Representatives

April 19, 2016

TAX FILING

IRS Needs a Comprehensive Customer Service Strategy and Needs to Better Combat Identity Theft Refund Fraud and Protect Taxpayer Data

Why GAO Did This Study

IRS provides service to tens of millions of taxpayers and processes most tax returns during the filing season. It is also a time when legitimate taxpayers may learn that they are a victim of IDT refund fraud, which occurs when a thief files a fraudulent return using a legitimate taxpayer's identity and claims a refund. In 2015, GAO added IDT refund fraud to its high-risk area on the enforcement of tax laws and expanded its government-wide high-risk area on federal information security to include the protection of personally identifiable information. With IRS's reliance on computerized systems, recent data breaches at IRS highlight the vulnerability of sensitive taxpayer information.

This statement discusses IRS's efforts to address (1) customer service declines, (2) IDT refund fraud challenges, and (3) information security weaknesses. This statement is based on GAO reports issued between 2012 and 2016 and includes updates of selected data.

What GAO Recommends

GAO previously suggested that Congress consider requiring that Treasury work with IRS to develop a customer service strategy, and providing Treasury with the authority to lower the annual threshold for e-filing W-2s. GAO made prior recommendations to IRS to combat IDT refund fraud, such as assessing the costs, benefits, and risks of taxpayer authentication options, and 45 new recommendations to further improve IRS's information security controls and the implementation of its agency-wide information security program.

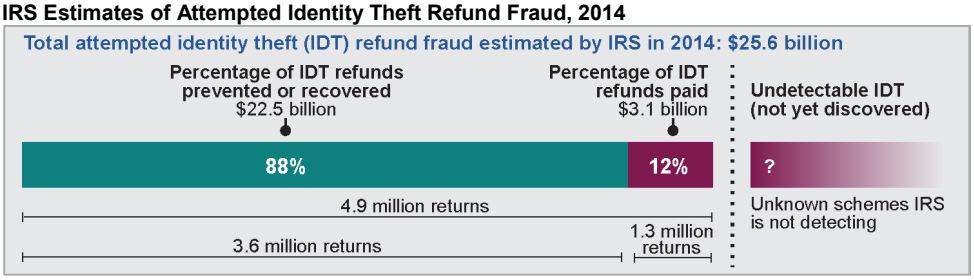
View GAO-16-578T. For more information, contact Jessica K. Lucas-Judy at (202) 512-9110 or LucasJudyJ@gao.gov, or Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

The Internal Revenue Service (IRS) improved phone service to taxpayers during the 2016 filing season compared to last year. According to IRS, this is due in part to the additional $290 million in funding Congress provided to improve customer service, identity theft (IDT) refund fraud, and cybersecurity efforts. However, IRS expects its performance for the entire fiscal year will not reach the levels of earlier years. In 2012 and 2014, GAO made recommendations for IRS to improve customer service, which it has yet to implement. Consequently, in December 2015, GAO suggested that Congress require the Department of the Treasury (Treasury) to work with IRS to develop a comprehensive customer service strategy that incorporates elements of these prior recommendations.

IDT refund fraud poses a significant challenge. Although the full extent of this fraud is unknown, IRS estimates it paid $3.1 billion in IDT fraudulent refunds in filing season 2014, while preventing the processing of $22.5 billion in fraudulent refunds (see figure).

IRS Estimates of Attempted Identity Theft Refund Fraud, 2014



Source: GAO analysis of IRS data. | GAO-16-578T

IRS has taken steps to combat IDT refund fraud, such as increasing resources dedicated to combating the problem. However, as GAO reported in August 2014 and January 2015, additional actions can further assist the agency, including assessing the costs, benefits, and risks of improving methods for authenticating taxpayers. In addition, the Consolidated Appropriations Act, 2016 included a provision to accelerate filings of W-2 information from employers to the IRS that would help IRS with pre-refund matching. GAO suggested that Congress provide Treasury with authority to lower the threshold for e-filing W-2s, which would further enhance pre-refund matching.

In March 2016, GAO reported that IRS had instituted numerous controls over key financial and tax processing systems; however, it had not always effectively implemented other controls intended to properly restrict access to systems and information, among other security measures. While IRS had improved some of its access controls, weaknesses remained in controls over key systems for identifying and authenticating users, authorizing users' level of rights and privileges, and encrypting sensitive data. These weaknesses were due in part to IRS's inconsistent implementation of its agency-wide security program, including not fully implementing 49 prior GAO recommendations. GAO concluded that these weaknesses collectively constituted a significant deficiency for the purposes of financial reporting for fiscal year 2015. As a result, taxpayer and financial data continue to be exposed to increased risk.

Chairman Roskam, Ranking Member Lewis, and Members of the Subcommittee:

Thank you for the opportunity to testify on the Internal Revenue Service's (IRS) 2016 filing season performance, identity theft (IDT) refund fraud and information security.

The filing season—which ended yesterday for most of the country—is the time when millions of taxpayers contact IRS over the phone, through written correspondence, in person, and via IRS's website.[1] It is also during this period that IRS processes most of the approximately 150 million individual tax returns it will receive, conducts initial screening for compliance, and issues more than 100 million refunds. The scale of these operations alone presents challenges, in addition to ensuring the security of taxpayers' personal and financial information. Customer service is one of those challenges.

Another major challenge for IRS during the filing season is the growing and evolving problem of IDT refund fraud and IRS efforts to prevent, detect, and resolve it. This crime occurs when a refund-seeking fraudster obtains an individual's Social Security number, date of birth, or other personally identifiable information (PII) and uses it to file a fraudulent tax return seeking a refund.[2] This crime costs the federal government billions of dollars in both IDT refunds paid to fraudsters and costs incurred by IRS in its efforts to combat it. Further, it burdens legitimate taxpayers because authenticating the victims' identities is likely to delay processing their returns and refunds, in those cases where a legitimate refund is due. Moreover, the victim's PII can potentially be used to commit other crimes. Given current and emerging risks, in 2015 we expanded the enforcement of our tax laws high-risk area to include IRS's efforts to address IDT refund fraud.[3]

[1]This year, most taxpayers had until April 18 to file a tax return with IRS.

[2]PII is information about an individual, including information that can be used to distinguish or trace their identity, such as name, Social Security number, mother's maiden name, or biometric records, as well as any other personal information that is linked or linkable to an individual. This statement discusses IDT refund fraud and not employment fraud. IDT employment fraud occurs when an identity thief uses a taxpayer's name and Social Security number to obtain a job.

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

In carrying out its mission to collect taxes, process tax returns, and enforce U.S. tax laws during the filing season and beyond, IRS relies extensively on computerized systems and on information security controls to protect the confidentiality, integrity, and availability of sensitive personal and financial information for each U.S. taxpayer. We first designated federal information security as a government-wide high-risk area in 1997. As we did with IDT refund fraud, in 2015 we expanded this area to include protecting the privacy of PII that is collected, maintained, and shared by both federal and nonfederal entities as a government-wide high-risk area.[4] Two recent information security incidents at IRS highlight the challenges and importance of ensuring that controls protecting taxpayer data are effectively implemented:

- In June 2015, the Commissioner of the IRS testified that unauthorized third parties had gained access to taxpayer information from its Get Transcript service.[5] According to IRS officials, criminals used taxpayer-specific data acquired from nondepartment sources to gain unauthorized access to information on approximately 100,000 tax accounts. These data included such PII as Social Security information, dates of birth, and street addresses. In an August 2015 update, IRS updated this number to be about 114,000, and reported that an additional 220,000 accounts had been inappropriately accessed. In a February 2016 update, the agency reported that an additional 390,000 accounts had been accessed. Thus, IRS has reported a total of about 724,000 accounts that were inappropriately accessed. The online Get Transcript service has been unavailable since May 2015.

- In March 2016, IRS stated that as part of its ongoing security review, it had temporarily suspended the Identity Protection Personal Identification Number (IP PIN) service on IRS.gov. The IP PIN is a single-use identification number provided to taxpayers who are victims

[4]GAO-15-290.

[5]The Get Transcript service provides users, via the IRS website, the ability to view, print, and download tax account, tax return, and record of account transcripts; wage and income documents; and proof of nonfiling transcripts. Taxpayers can also obtain transcripts by calling, writing, or walking into an IRS office.

of IDT to help prevent future IDT refund fraud.[6] The service on IRS's website allowed taxpayers to retrieve their IP PINs online. Taxpayers passed IRS's authentication checks by confirming their identities through site inquiries, asking for personal, financial, and tax-related information. The IRS stated that it was conducting further review of the IP PIN service and is looking at further strengthening the security features before resuming service. As of April 13, this online service was still suspended.

In response to challenges in these three areas, in fiscal year 2016, Congress provided IRS with $290 million in additional funding intended to improve customer service, IDT identification and prevention, and cybersecurity efforts.[7] According to IRS's spending plan this funding will be used to invest in (1) increased telephone level of service, including reduced wait times and improved performance on IRS's Taxpayer Protection Program/Identity Theft Toll Free Line ($178.4 million); (2) cybersecurity including network security improvements, protection from unauthorized access, and enhanced insider threat detection ($95.4 million); and (3) IDT refund fraud prevention ($16.1 million).

My statement today focuses on IRS's efforts to address (1) declines in customer service, (2) the challenge of identity theft refund fraud, and (3) information security weaknesses we have identified.

My statement is based in part on our previous reports issued between December 2012 and April 2016. Detailed descriptions of the scope and methodology for each of these reports can be found in each of the reports cited within this statement. We updated selected data in this statement with 2016 data from IRS on individual income tax return processing and telephone service, as well as IRS's fiscal year 2016 spending plan for the additional $290 million in appropriated funds. We also incorporated IRS statements on recent data breaches and IRS actions to address our past recommendations. To assess data reliability, we reviewed IRS data and

[6]In January 2014, IRS offered a limited IP PIN pilot program to eligible taxpayers in Florida, Georgia, and the District of Columbia. Taxpayers must confirm their identities with IRS to receive an IP PIN. IP PINs help prevent future IDT refund fraud because, once issued, the IP PIN must accompany their electronically filed tax return or else IRS will reject the return. If a paper return has a missing or incorrect IP PIN, IRS delays processing the return while the agency determines if it was filed by the legitimate taxpayer. See GAO, *Identity Theft: Additional Actions Could Help IRS Combat the Large, Evolving Threat of Refund Fraud*, GAO-14-633 (Washington, D.C.: Aug. 20, 2014), for more details on IRS's IP PIN service.

[7]Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, div. E, § 113, 129 Stat. 2242 (Dec. 18, 2015). Funding is available to IRS until September 30, 2017.

documentation and assessed it for data limitations. We found the data to be sufficiently reliable for our purposes. All the work on which this statement is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform our work 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.

IRS Improved its Telephone Service for the 2016 Filing Season but Still Needs to Develop a Comprehensive Customer Service Strategy

In addition to processing approximately 150 million individual tax returns and issuing more than 100 million refunds during the filing season, IRS provides a range of taxpayer services, including through telephones, written correspondence, and on its website.[8]

Based on recent data from IRS, compared to last year, IRS's telephone service has improved in the 2016 filing season. From January 1 through March 26, 2016, IRS received about 38.2 million calls to its automated and live assistor telephone lines—a slight decrease compared to the same period last year.[9] Of the 14.7 million calls seeking live assistance, IRS had answered 9.9 million calls—a 72 percent increase over the 5.7 million calls answered during the same period last year. Further, the average wait time to speak to an assistor also decreased from 24 to 10 minutes.

IRS anticipated that 65 percent of callers seeking live assistance would receive it this filing season, which ended April 18. IRS's performance for telephone service during the filing season as of March 26, 2016 has exceeded IRS's anticipated level—74 percent of callers have received live assistance.

[8]The filing season generally runs between January and mid-April.

[9]Total call volume to IRS's toll free telephone lines include automated and assistor calls answered, as well as those that received a busy signal or were abandoned or disconnected.

IRS attributed this year's improvements to a number of factors. As noted above, of the additional $290 million IRS received in December 2015, it allocated $178.4 million (61.5 percent) for taxpayer services to make measurable improvements in its telephone level of service. With the funds, IRS hired 1,000 assistors who began answering taxpayer calls in March, in addition to the approximately 2,000 seasonal assistors it had hired in fall 2015.[10] To help answer taxpayer calls before March, IRS officials told us that they detailed 275 staff from one of its compliance functions to answer telephone calls.[11] IRS officials said they believe this step was necessary because the additional funding came too late in the year to hire and train assistors to fully cover the filing season. IRS also plans to use about 600 full-time equivalents of overtime for assistors to answer telephone calls and respond to correspondence in fiscal year 2016. This compares to fewer than 60 full-time equivalents of overtime used in fiscal year 2015.

However, IRS expects that the telephone level of service will decline after the filing season. As a result, the telephone level of service for the entire 2016 fiscal year is expected to be at 47 percent.[12] As we reported in March 2016, IRS's telephone level of service for the fiscal year has yet to reach the levels it had achieved in earlier years (see figure 1).[13]

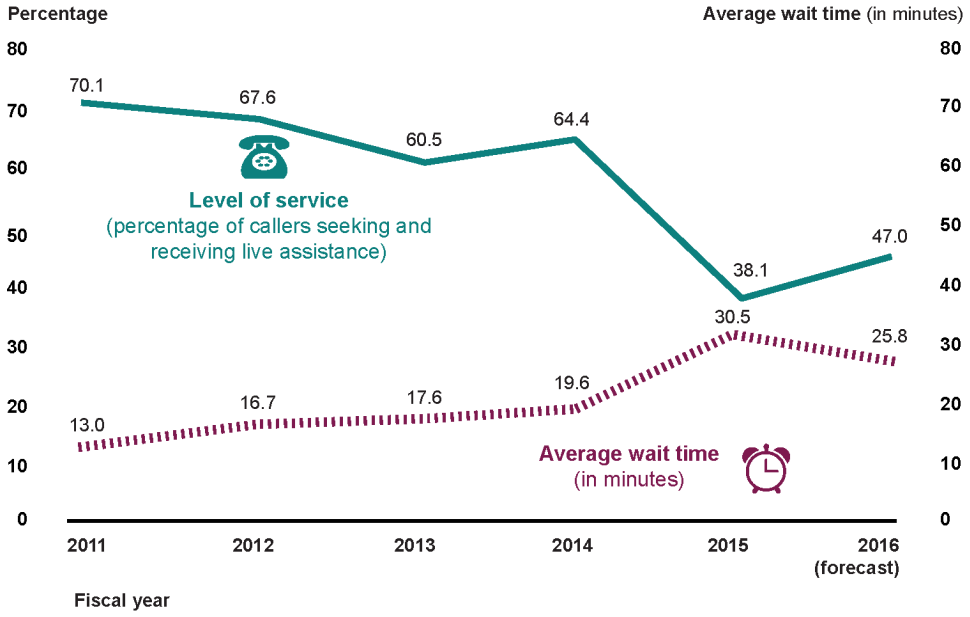
[10]In contrast, IRS reduced the number of assistors answering telephone calls between fiscal years 2010 and 2015, which contributed to the lowest level of telephone service in fiscal year 2015 compared to recent years.

[11]IRS has not yet determined the amount of foregone revenue from taking this action.

[12]IRS's projected telephone level of service for the filing season covers the period between January 1, 2016 and April 23, 2016.

[13]GAO, *Internal Revenue Service: Preliminary Observations on the Fiscal Year 2017 Budget Request and 2016 Filing Season Performance*, GAO-16-459R (Washington, D.C.: Mar. 8, 2016).

Figure 1: IRS Telephone Level of Service and Average Telephone Wait Time, Fiscal Year 2011 through Fiscal Year 2016 Performance Forecast



Source: GAO analysis of IRS data. | GAO-16-578T

In addition to answering telephone calls, IRS responds to millions of letters and other correspondence from taxpayers. In 2015, we reported that the percentage of correspondence cases in IRS's inventory classified as "overage"—cases generally not processed within 45 days of receipt by IRS—has stayed close to 50 percent since fiscal 2013.[14] Minimizing overaged correspondence is important because delayed responses may prompt taxpayers to write again, call, or visit a walk-in site. Moreover, an increasing overage rate could lead to more interest paid to taxpayers who are owed refunds.

In March 2016, IRS officials attributed improvements made this filing season, in part, to assistors working overtime. These officials reported that IRS's office that responds to taxpayer inquiries and handles

[14]IRS can classify correspondence in its inventory as "overage" from 30 to 180 days after IRS receives them depending on the type of work performed by assistors. For example, correspondence cases generated internally age 75 days from the date IRS receives such cases, while international adjustment cases generated by taxpayers age 90 days from the date IRS receives them. See GAO, *2015 Tax Filing Season: Deteriorating Taxpayer Service Underscores Need for a Comprehensive Strategy and Process Efficiencies,* GAO-16-151 (Washington, D.C.: Dec. 16, 2015).

adjustments had slightly more than 700,000 correspondence cases in inventory at the end of January and expect about 1 million cases in inventory by the end of April. They described IRS's correspondence inventory as manageable, but steadily increasing. Officials said that, after the filing deadline, assistors will turn their attention to correspondence.

IRS also offers online services to millions of taxpayers through its website, including tax forms and interactive tax assistance features. According to IRS, the agency wants to expand online service to provide greater convenience to taxpayers which has the potential to reduce costs in other areas, such as its telephone operations.

Implementing Our Prior Recommendations Could Help IRS Improve Customer Service

We have made recommendations to IRS and the Department of the Treasury (Treasury), as well as a matter for congressional consideration, to assist IRS in improving its customer service. Examples include:

Telephone and Correspondence. In December 2012, we recommended that IRS define appropriate levels of service for telephones as well as correspondence.[15] IRS neither agreed nor disagreed with this recommendation and, as of October 2015, the agency had not developed these customer service goals. While IRS has taken some steps to modify services provided to taxpayers, a strategy would help determine the resources needed to achieve customer service goals. Recognizing the importance of such as strategy, in December 2014, we recommended that IRS systematically and periodically compare its telephone service to the best in business to identify gaps between actual and desired performance.[16] IRS disagreed with this recommendation, noting that it is difficult to identify comparable organizations. We do not agree with IRS's position; many organizations run call centers that would provide ample opportunities to benchmark IRS's performance.

Recognizing the need to improve performance responding to taxpayer correspondence, in December 2015, we recommended to Treasury that it include overage rates for handling taxpayer correspondence as a part of

[15]GAO, *2012 Tax Filing: IRS Faces Challenges Providing Service to Taxpayers and Could Collect Balances Due More Effectively,* GAO-13-156 (Washington, D.C.: Dec. 18, 2012).

[16]GAO, *Tax Filing Season: 2014 Performance Highlights the Need to Better Manage Taxpayer Service and Future Risks,* GAO-15-163 (Washington, D.C.: Dec. 16, 2014).

Treasury's performance goals. Treasury neither agreed nor disagreed with this recommendation.

Online Services. In April 2013, we recommended that IRS develop a long-term online strategy that should, for example, develop business cases for all new online services.[17] In March 2016, IRS officials reported that IRS's Future State initiative is intended to provide better service to taxpayers through multiple channels of communication, including online.[18] We have not yet assessed IRS's Future State initiative. However, a long-term comprehensive strategy for online services should help ensure that IRS is maximizing the benefit to taxpayers from this investment and reduce costs in other areas, such as for IRS's telephone operations.

Comprehensive Customer Service Strategy. In fall 2015, Treasury and IRS officials said they had no plans to develop a comprehensive customer service strategy or specific goals for telephone service tied to the best in the business and customer expectations. These officials told us that the agencies' existing efforts were sufficient. However, we continue to believe that, without such a strategy, Treasury and IRS can neither measure nor effectively communicate to Congress the types and levels of customer service taxpayers should expect and the resources needed to reach those levels. Therefore, in December 2015, we suggested that Congress consider requiring that Treasury work with IRS to develop a comprehensive customer service strategy.[19] In April 2016, IRS officials told us that the agency has established a team to consider our prior recommendations in developing a comprehensive customer service strategy or goals for telephone service.

Billions of Dollars Have Been Lost to IDT Refund Fraud, and IRS Faces Challenges in Combating This Evolving Threat

During the filing season many taxpayers learn that their private information has been stolen and they have been victims of IDT refund fraud. This generally occurs when the taxpayer attempts to file a tax

[17]GAO, *IRS Website: Long-Term Strategy Needed to Improve Interactive Services,* GAO-13-435 (Washington, D.C.: Apr. 16, 2013).

[18]According to IRS, the agency is working to transform its operations in order to modernize the taxpayer experience and empower its workforce to operate more efficiently—which will make filing simpler for taxpayers and increase voluntary compliance.

[19]GAO-16-151.

return only to learn that one has already been filed under the taxpayer's name. For these taxpayers, IRS has taken action to improve customer service related to IDT refund fraud. As we reported in March 2016, between the 2011 and 2015 filing seasons, IRS experienced a 430 percent increase in the number of telephone calls to its Identity Theft Toll-Free Line.[20] As of March 19, 2016, IRS had received more than 1.1 million calls to this line.[21] During this time, 77 percent of callers seeking assistance on this telephone line received it compared to 54 percent during the same period last year. Average wait times during the same period have also decreased—taxpayers were waiting an average of 14 minutes to talk to an assistor, a decrease from 27 minutes last year.

As we reported in April 2016, billions of dollars have been lost to IDT refund fraud and this crime continues to be an evolving threat.[22] IRS develops estimates of the extent of IDT refund fraud to help direct its efforts to identify and prevent the crime. While its estimates have inherent uncertainty, IRS estimated that it prevented or recovered $22.5 billion in fraudulent IDT refunds in filing season 2014 (see figure 2).[23] However, IRS also estimated, where data were available, that it paid $3.1 billion in fraudulent IDT refunds. Because of the difficulties in knowing the amount of undetectable fraud, the actual amount could differ from these estimates.

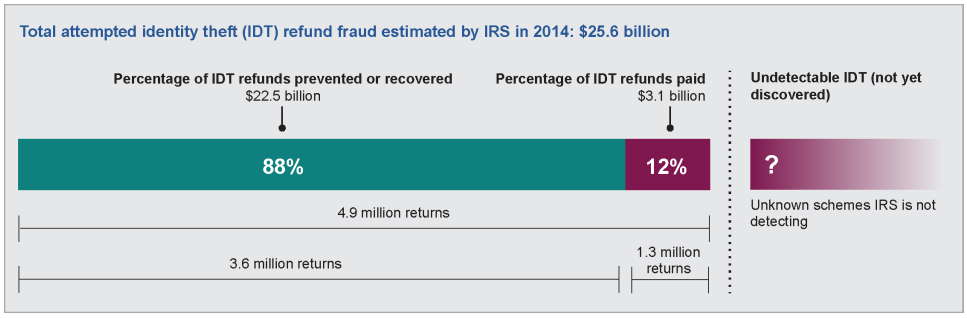
[20]GAO-16-459R.

[21]Total call volume to IRS's identity theft protection toll-free telephone line includes automated and assistor calls answered, as well as those that received a busy signal or were abandoned or disconnected.

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

[23]IRS's 2014 estimates cannot be compared to 2013 estimates because of substantial methodology changes to better reflect new IDT refund fraud schemes and to improve the accuracy of its estimates, according to IRS officials. We are reviewing IRS's IDT refund fraud estimates as part of ongoing work.

Figure 2: IRS Estimates of Attempted Identity Theft Refund Fraud, 2014



Source: GAO analysis of IRS data. | GAO-16-578T

IRS has taken steps to address IDT refund fraud; however, it remains a persistent and continually changing threat. IRS recognized the challenge of IDT refund fraud in its fiscal year 2014-2017 strategic plan and increased resources dedicated to combating IDT and other types of refund fraud.[24] In fiscal year 2015, IRS reported that it staffed more than 4,000 full-time equivalents and spent about $470 million on all refund fraud and IDT activities.[25] As described above, IRS received an additional $290 million in fiscal year 2016 to improve customer service, IDT identification and prevention, and cybersecurity efforts. The agency plans to use $16.1 million of this funding to help prevent IDT refund fraud, among other things. As we reported in April 2016, the administration requested an additional $90 million and an additional 491 full-time equivalents for fiscal year 2017 to help prevent IDT refund fraud and reduce other improper payments.[26] IRS estimates that this $90 million investment in IDT refund fraud and other improper payment prevention would help it protect $612 million in revenue in fiscal year 2017, as well as protect revenue in future years.

As we previously reported, IRS also works with third parties, such as tax preparation industry participants, states, and financial institutions to try to

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

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

[26]See GAO-16-375SP. Improper payments are payments that should not have been made or that were made in an incorrect amount (including overpayments and underpayments).

detect and prevent IDT refund fraud.[27] In March 2015, the Commissioner of the IRS convened a Security Summit with industry and states to improve information sharing and authentication. IRS officials said that 40 state departments of revenue and 20 tax industry participants have officially signed a partnership agreement to enact recommendations developed and agreed to by summit participants. IRS plans to invest a portion of the $16.1 million it received in fiscal year 2016 into identity theft prevention and refund fraud mitigation actions from the Security Summit. These efforts include developing an Information Sharing and Analysis Center where IRS, states, and industry can share information to combat IDT refund fraud.

Even though IRS has prioritized combating IDT refund fraud, fraudsters adapt their schemes to identify weaknesses in IDT defenses, such as gaining access to taxpayers' tax return transcripts through IRS's online Get Transcript service.[28] According to IRS officials, with access to tax transcripts, fraudsters can create historically consistent returns that are hard to distinguish from a return filed by a legitimate taxpayer. This can make it more difficult for IRS to identify and detect IDT refund fraud.

Stronger Pre-refund and Post-refund Strategies Can Help Combat IDT Refund Fraud

Because identity thieves are "adaptive adversaries" who are constantly learning and changing their tactics as IRS develops new IDT strategies, IRS will need stronger pre-refund and post-refund strategies to combat this persistent and evolving threat. While there are no simple solutions, our past work has highlighted ways IRS can combat this threat.

Improved authentication. Improving authentication could help IRS prevent fraud before issuing refunds. In January 2015, we reported that IRS's authentication tools have limitations and recommended that IRS assess the costs, benefits and risks of its authentication tools.[29] For

[27]GAO, *Information Security: IRS Needs to Further Improve Controls over Taxpayer Data and Continue to Combat Identity Theft Refund Fraud*, GAO-16-589T (Washington, D.C.: Apr. 12, 2016).

[28]As mentioned above, the online Get Transcript service has been unavailable since May 2015.

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

example, individuals can obtain an e-file PIN by providing their name, Social Security number, date of birth, address, and filing status for IRS's e-file PIN application. Identity thieves can easily find this information, allowing them to bypass some, if not all, of IRS's automatic checks according to our analysis and interviews with tax software and return preparer associations and companies. After filing an IDT return using an e-file PIN, the fraudulent return would proceed through IRS's normal return processing.

In response to our recommendation, in November 2015, IRS developed guidance for its Identity Assurance Office to assess costs, benefits, and risk. According to IRS officials, this analysis will inform decision-making on authentication-related issues. IRS also noted that the methods of analysis for the authentication tools will vary depending on the different costs and other factors for authenticating taxpayers in different channels, such as online, phone, or in-person. In February 2016, IRS officials told us that the Identity Assurance Office plans to complete a strategic plan for taxpayer authentication across the agency in September 2016. While IRS is taking steps, it will still be vulnerable until it completes and uses the results of its analysis of costs, benefits, and risks to inform decision-making.

W-2 Pre-refund Matching. Another pre-refund strategy is earlier matching of employer-reported wage information to taxpayers' returns before issuing refunds. As we reported in August 2014, thieves committing IDT refund fraud take advantage of IRS's "look-back" compliance model.[30] Under this model, rather than holding refunds until completing all compliance checks, IRS issues refunds after conducting selected reviews, such as verifying identity by matching names and Social Security numbers and filtering for indications of fraud.[31] However, we found that the wage information that employers report on the Form W-2, *Wage and Tax Statement* (W-2), has generally been unavailable to IRS until after it issues most refunds. According to IRS, pre-refund matching would potentially save a substantial part of the billions of taxpayer dollars currently lost to fraudsters.

[30]GAO-14-633.

[31]These reviews can detect inconsistencies, allowing IRS to resolve any issues and—in some cases—prevent refunds.

- *Increasing electronically-filed (e-file) W-2s.* In December 2015, the Consolidated Appropriations Act, 2016 amended the tax code to accelerate W-2 filing deadlines to January 31.[32] This represents important progress. Building on that, other policy changes may also be needed in concert with moving W-2 deadlines. Agency officials and third-party stakeholders told us that these changes include lowering the employee threshold requirement for employers to e-file W-2s.[33] Because of the additional time and resources associated with processing paper W-2s submitted by employers, Social Security Administration officials told us that a change in the e-file threshold would be needed to sufficiently increase the number of e-filed W-2s. Backlogs in paper W-2s could result in IRS receiving W-2 data after the end of the filing season. Therefore, we have suggested that Congress should consider providing the Secretary of the Treasury with the regulatory authority to lower the threshold for electronic filing of W-2s from 250 returns annually to between 5 to 10 returns, as appropriate.

- *Assessing the costs and benefits of pre-refund W-2 matching.* In August 2014 we reported that the wage information that employers report on Form W-2 is unavailable to IRS until after it issues most refunds.[34] Also, if IRS had access to W-2 data earlier, it could match such information to taxpayers' returns and identify discrepancies before issuing billions of dollars of fraudulent IDT refunds. We recommended that IRS assess the costs and benefits of accelerating W-2 deadlines.

  In response to our recommendation, IRS provided us with a report in September 2015 discussing (1) adjustments to IRS systems and work processes needed to use accelerated W-2 information, (2) the potential impacts on internal and external stakeholders, and (3) other changes needed to match W-2 data to tax returns prior to issuing refunds, such as delaying refunds until W-2 data

[32]Pub. L. No. 114-113, div. Q, § 201, 129 Stat. 2242 (Dec. 18, 2015). This change goes into effect for W-2s reporting payments made in 2016 and filed in 2017.

[33]Currently, employers who file 250 or more W-2s annually must electronically file those forms. 26 C.F.R. § 301.6011-2(b)(2). IRS is generally prohibited from requiring those filing fewer than 250 returns annually to e-file. 26 U.S.C. § 6011(e)(2)(A). For details, see GAO-14-633.

[34]GAO-14-633.

are available. IRS's analysis for this report will help it determine how to best implement pre-refund W-2 matching, given the new January 31 deadline for filing W-2s.

Improving feedback on external leads. A post-refund strategy to combat IDT refund fraud involves IRS's External Leads Program. This program involves financial institutions and other external parties providing information about emerging IDT refund trends and fraudulent returns that have passed through IRS detection systems. In August 2014, we reported that IRS provided limited feedback to external parties on IDT leads they submitted and offered external parties limited general information on IDT refund fraud trends. We recommended that IRS provide actionable feedback to all lead-generating third parties, and IRS neither agreed nor disagreed.[35]

However, in response to our recommendation, IRS took a number of steps. First, in November 2015, IRS reported that it had developed a database to track leads submitted by financial institutions and the results of those leads. IRS also stated that it had held two sessions with financial institutions to provide feedback on external leads provided to IRS. Second, in December 2015, IRS officials told us that the agency sent a customer satisfaction survey asking financial institutions for feedback on the external leads process. The agency was also considering other ways to provide feedback to financial institutions. Third, in April 2016, IRS officials told us that they plan to analyze preliminary survey results by mid-April 2016. Finally, IRS officials reported that the agency shared information with financial institutions in March 2016 and plans to do so on a quarterly basis. The next information sharing session is scheduled in June 2016. We are following up with IRS on these activities to determine the extent to which IRS has addressed our recommendation.

[35]GAO-14-633.

Although IRS Has Made Improvements, Information Security Weaknesses Continue to Place Taxpayer and Financial Data at Risk

In addition to securing taxpayer information to help prevent IDT refund fraud, there are additional concerns for maintaining security of taxpayer data. As we reported in March 2016,[36] IRS has implemented numerous controls over key financial and tax processing systems; however, it had not always effectively implemented access and other controls,[37] including elements of its information security program.

Access controls are intended to prevent, limit, and detect unauthorized access to computing resources, programs, information, and facilities. These controls include identification and authentication, authorization, cryptography, audit and monitoring, and physical security controls, among others. In our most recent review in March 2016, we found that IRS had improved access controls, but some weaknesses remain.[38] Examples include:

- **Identifying and authenticating** users—such as through user account-password combinations—provides the basis for establishing accountability and controlling access to a system. IRS established policies for identification and authentication, including requiring multifactor authentication for local and network access accounts, and establishing password complexity and expiration requirements.[39] It also improved identification and authentication controls by, for example, expanding the use of an automated mechanism to centrally manage, apply, and verify password requirements. However,

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

[37]Information security controls include logical and physical access controls, configuration management, and continuity of operations. These controls are designed to ensure that access to data is properly restricted, physical access to sensitive computing resources and facilities is protected, systems are securely configured to avoid exposure to known vulnerabilities, and backup and recovery plans are adequate and tested to ensure the continuity of essential operations.

[38]GAO-16-398.

[39]Multifactor authentication involves using two or more factors to achieve authentication. Factors include something you know (password or personal identification number), something you have (cryptographic identification device or token), or something you are (biometric).

weaknesses in identification and authentication controls remained. For example, the agency used easily guessable passwords on servers supporting key systems.

- **Authorization controls** limit what actions users are able to perform after being allowed into a system. They should be based on the concept of "least privilege," granting users the least amount of rights and privileges necessary to perform their duties. While IRS established policies for authorizing access to its systems, we found that it continued to permit excessive access in some cases. For example, users were granted rights and permissions in excess of what they needed to perform their duties, including for an application used to process electronic tax payment information and a database on a human resources system.

- **Cryptography controls** protect sensitive data and computer programs by rendering data unintelligible to unauthorized users and protecting the integrity of transmitted or stored data. IRS policies require the use of encryption and it continued to expand its use of encryption to protect sensitive data. However, key systems we reviewed had not been configured to encrypt sensitive user authentication data.

IRS also had weaknesses in configuration management controls, which are intended to prevent unauthorized changes to information system resources (e.g., software and hardware), and provide assurance that systems are configured and operating securely. Specifically, while IRS developed policies for managing the configuration of its information technology (IT) systems and improved some configuration management controls, it did not, for example, ensure security patch updates were applied in a timely manner to databases supporting two key systems we reviewed, including a patch that had been available since August 2012.

To its credit, IRS had established contingency plans for the systems we reviewed, which help ensure that when unexpected events occur, critical operations can continue without interruption or can be promptly resumed, and that information resources are protected. Specifically, IRS had established policies for developing contingency plans for its information systems and for testing those plans, as well as for implementing and enforcing backup procedures. Moreover, the agency had documented and tested contingency plans for its systems and improved continuity of operations controls for several systems.

Nevertheless, the control weaknesses we found can be attributed in part to IRS's inconsistent implementation of elements of its agency-wide information security program. The agency established a comprehensive framework for its program, including assessing risk for its systems, developing system security plans, and providing employees with security awareness and specialized training. However, IRS had not updated key mainframe policies and procedures to address issues such as comprehensively auditing and monitoring access.

In addition, the agency had not fully addressed previously identified deficiencies or ensured that its corrective actions were effective. During our most recent review, IRS told us it had addressed 28 of our prior recommendations; however, we determined that 9 of these had not been effectively implemented.

We concluded in our November 2015 report that the collective effect of the deficiencies in information security from prior years that continued to exist in fiscal year 2015, along with the new deficiencies we identified, were serious enough to merit the attention of those charged with governance of IRS and therefore represented a significant deficiency in IRS's internal control over financial reporting systems as of September 30, 2015.[40]

Implementing GAO Recommendations Can Help IRS Better Protect Sensitive Taxpayer and Financial Data

To assist IRS in fully implementing its agency-wide information security program, we made two new recommendations to more effectively implement security-related policies and plans.[41] In addition, to assist IRS in strengthening security controls over the financial and tax processing systems we reviewed, we made 43 technical recommendations in a

[40]A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit the attention of those charged with governance. A material weakness is a deficiency, or combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis. A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. For additional information, see GAO, *Financial Audit: IRS's Fiscal Years 2015 and 2014 Financial Statements*, GAO-16-146 (Washington, D.C.: Nov. 12, 2015).

[41]GAO-16-398.

separate report with limited distribution to address 26 new weaknesses in access controls and configuration management.[42]

Implementing these recommendations—in addition to the 49 outstanding recommendations from previous audits—will help IRS improve its controls for identifying and authenticating users. This, in turn, will allow IRS to limit users' access to the minimum necessary to perform their job-related functions, protect sensitive data when they are stored or in transit, audit and monitor system activities, and physically secure its IT facilities and resources.

In commenting on drafts of our reports presenting the results of our fiscal year 2015 audit, the IRS Commissioner stated that while the agency agreed with our new recommendations, it will review them to ensure that its actions include sustainable fixes that implement appropriate security controls balanced against IT and human capital resource limitations.

In conclusion, this year's tax filing season has generally gone smoothly and IRS has improved customer service. While IRS has some initiatives to review customer service and consider improvements, it still needs to develop a comprehensive strategy for customer service that will meet the needs of taxpayers. This strategy could include setting customer service goals as well as benchmarking and monitoring performance.

IRS also needs to strengthen its defenses for addressing IDT refund fraud that is informed by assessing the cost, benefits, and risks of IRS's various authentication options.

Finally, weaknesses in information security can also increase the risk posed by IDT refund fraud. While IRS has made progress in implementing information security controls, it needs to continue to address weaknesses in access controls and configuration management and consistently implement all elements of its information security program. The risks to which the IRS and the public are exposed have been illustrated by recent incidents involving public-facing applications, highlighting the importance of securing systems that contain sensitive taxpayer and financial data.

Chairman Roskam, Ranking Member Lewis, and Members of the Subcommittee, this concludes my statement. I look forward to answering any questions that you may have at this time.

[42]GAO, *Information Security: IRS Needs to Further Improve Controls over Financial and Taxpayer Data*, GAO-16-397SU (Washington, D.C.: Mar. 28, 2016).

Contacts and Staff Acknowledgments

If you have any questions regarding this statement, please contact Jessica K. Lucas-Judy at (202) 512-9110 or LucasJudyJ@gao.gov, James R. McTigue, Jr. at (202) 512-9110 or mctiguej@gao.gov, Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov, or Nancy Kingsbury at (202) 512-2928 or kingsburyn@gao.gov. Other key contributors to this statement include Neil A. Pinney, Joanna M. Stamatiades, and Jeffrey Knott, (assistant directors); Dawn E. Bidne; Mark Canter; James Cook; Shannon J. Finnegan; Lee McCracken; Justin Palk; J. Daniel Paulk; Erin Saunders Rath; and Daniel Swartz.