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 10:45 a.m.
Wednesday, September 26, 2018

IDENTITY THEFT

Strengthening Taxpayer Authentication Efforts Could Help Protect IRS Against Fraudsters

Statement of James R. McTigue, Jr., Director, Strategic Issues

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

I am pleased to be here today to discuss the Internal Revenue Service's (IRS) efforts to monitor and improve taxpayer authentication. In fiscal year 2017, IRS issued approximately $383 billion in individual tax refunds, including overpayment refunds and refundable tax credits, an increase of about $16 billion from the previous fiscal year. In an environment with an increasing risk of fraud, identity theft (IDT), and cyberattacks, IRS must ensure that its preventative security controls provide the agency with reasonable assurance that it is interacting with the legitimate taxpayer. Authentication—the process by which IRS verifies taxpayers are who they claim to be—is a critical step in both protecting sensitive taxpayer information and preventing potentially billions of dollars of refunds from being paid to fraudsters each year. According to IRS's most recent data, it estimates that in 2016, at least $12.2 billion in IDT tax refund fraud was attempted; of this amount, at least $1.6 billion was paid out to fraudsters.

IRS's ability to continuously monitor its current authentication methods while also looking ahead to new identity verification technologies is critical to keeping ahead of fraudsters, who constantly adapt their schemes to thwart IRS's defenses. The agency must also strike a balance in designing its authentication programs. Authentication must be strong enough to prevent fraudsters from gaining access to IRS services using stolen personally identifiable information, without being overly burdensome on legitimate taxpayers who also must authenticate.

My remarks today highlight selected findings of our June 2018 report on IRS's efforts monitor and improve taxpayer authentication.[1] Specifically, this testimony addresses (1) IRS's efforts to address its authentication challenges, (2) IRS's progress in implementing its authentication strategy, and (3) additional steps we identified that IRS could take to enhance its authentication programs and stay ahead of fraudsters.

To conduct the work for our June report, we reviewed IRS documents and information related to taxpayer authentication including authentication policies, risk assessments, and performance metrics. We compared IRS's authentication efforts to applicable activities in the *IRS Identity Assurance*

[1]GAO, *Identity Theft: IRS Needs to Strengthen Taxpayer Authentication Efforts,* GAO-18-418 (Washington, D.C.: June 22, 2018).

Strategy and Roadmap (Roadmap), Standards for Internal Control in the Federal Government, and relevant National Institute of Standards and Technology (NIST) guidance, among others.[2] We also interviewed IRS officials knowledgeable about the agency's taxpayer authentication programs, as well as IRS, state, and industry co-leads from two Security Summit workgroups to understand IRS's collaborative efforts to improve taxpayer authentication.[3] To assess how IRS can improve its authentication programs going forward, we met with knowledgeable officials from NIST to discuss its guidelines for online identity-proofing and authentication. We also compared IRS's authentication programs and plans for future improvements to its *Roadmap*, federal internal controls, guidance from NIST and the Office of Management and Budget (OMB), principles for project planning, and our prior work on information technology investment management and cost estimating. We also interviewed officials from three other federal agencies and a nongeneralizable selection of representatives from state revenue offices, industry, and financial institutions to understand the range of authentication technologies other organizations are using. Our report includes a detailed explanation of the methods used to conduct our work. The work on which this testimony is based was performed in accordance with generally accepted government auditing standards.

In brief, Madam Chairman, our work found that IRS has taken some steps to improve taxpayer authentication, including working with external partners to identify solutions for combating IDT refund fraud and developing an authentication strategy to address its most pressing authentication challenges. However, we also found that IRS has not prioritized the initiatives supporting its authentication strategy nor identified the resources required to complete them. Further, we found that IRS does not have clear plans and timelines to fully implement NIST's new guidance for secure online authentication and also lacks a comprehensive process to evaluate potential new authentication technologies, which could provide taxpayers additional options to actively

[2]GAO, *Standards for Internal Control in the Federal Government,* GAO-14-704G (Washington, D.C.: September 2014); and *A Framework for Managing Fraud Risks in Federal Programs,* GAO-15-593SP (Washington, D.C.: July 28, 2015). National Institute of Standards and Technology, *Electronic Authentication Guideline*, *Special Publication 800-63-2,* (August 2013), superseded by *Digital Identity Guidelines, Special Publication 800-63-3* (June 2017).

[3]The Security Summit is an ongoing effort between IRS, industry and states to address IDT challenges.

protect their identity. We made 11 recommendations to address these and other weaknesses identified in our report. IRS agreed with all 11 recommendations and stated that it is taking action to address them.

IRS Has Broad Efforts Underway to Address Authentication Challenges

Our report noted that IRS has established organizational structures essential to supporting its taxpayer authentication efforts. Specifically, IRS created an Identity Assurance Office (IAO) in 2015 to work with stakeholders across IRS to review and assess the agency's various authentication programs and efforts. In 2016, IAO led an effort that identified over 100 interactions between IRS and taxpayers that require authentication and categorized these interactions based on potential risks to the agency and taxpayers. Further, in December 2016, IAO released its *Roadmap* for developing a modern and secure authentication environment for all taxpayers regardless of how they interact with IRS—online, over the telephone, in person, or via correspondence.

We also found that IRS is working to address its authentication challenges by collaborating with industry members and state partners via the Security Summit. The Security Summit was established in 2015 as an ongoing effort between industry experts from tax software companies, paid preparers, financial institutions, and states to improve information sharing and fraud detection and to address common IDT challenges. The Security Summit's authentication workgroup leads several initiatives aimed at verifying the authenticity of the taxpayer and the tax return at the time of filing. One initiative involves analyzing data elements—such as trusted customer requirements and other characteristics of the return—that are collected during the tax return preparation and electronic filing process. In addition, in 2016 the authentication workgroup recommended improved account password standards to help protect taxpayers' accounts from being taken over by criminals.

Overall, we found that officials—representing IRS, industry, and states—expressed positive views about the level of commitment and cooperation guiding the group's authentication efforts. Officials with whom we spoke stated that they are dedicated to continuing to address authentication issues collaboratively because they have a mutual interest in improving authentication to reduce tax refund fraud.

IRS Has Begun to Implement Its Authentication Strategy, but Has Not Articulated Priorities and Resource Needs

In its *Roadmap*, IRS outlined six core authentication objectives, 10 high-level strategic efforts, and 14 foundational initiatives to help it address authentication challenges and identify opportunities for future investment. While we found that IRS has made progress on some efforts identified in its *Roadmap*, it has not prioritized the initiatives supporting its strategy nor identified the resources required to complete them, consistent with program management leading practices.

For example, one of IRS's foundational initiatives is to send event-driven notifications to taxpayers, such as when they file a return or request a tax transcript. Such notifications could help IRS and taxpayers detect potentially fraudulent activity at the earliest stage and help improve authentication of tax returns. The *Roadmap* identifies seven supporting activities for this foundational initiative. One is to provide taxpayers with greater control over their online accounts. Another supporting activity is to determine methods for sending notifications to taxpayers about activity on their account.[4]

However, IRS has not identified the resources required to complete these activities, and the *Roadmap* notes that six of the seven activities will take between 6 months to 3 years to complete. In December 2017, IRS officials stated that they had developed business requirements for the foundational initiative to give taxpayers greater control over their online accounts. However, IRS has not identified funding for the initiative's other supporting activities—such as developing requirements to send push notifications to taxpayers—and implementation will depend on the availability of future resources.[5]

In December 2017, IRS officials stated that each of the strategic efforts and foundational initiatives identified in the *Roadmap* are a high priority, and they are working to address them concurrently while balancing the availability of resources against the greatest threats to the tax environment. As noted in our report, we recognize that a strategy is necessarily high-level and that IRS must remain flexible and use available

[4]According to IRS, notifications could be sent to the taxpayer via the IRS2Go application, text message, or e-mail. For example, the message could alert the taxpayer that a tax return was filed using the social security number associated with their online account.

[5]In January 2018, IRS officials noted that although this type of alert is not currently available, taxpayers can access their online account to review whether a return has been processed and filed for a current or prior tax year.

resources to respond to unexpected threats. Identifying resources and prioritizing activities in its *Roadmap* will help IRS clarify tradeoffs between costs, benefits, and risks and aid in decision making.

Further, such efforts may also help IRS establish clearer timelines and better respond to unexpected events. As such, we recommended that IRS estimate the resources (i.e., financial and human) required for the foundational initiatives and supporting activities identified in its *Roadmap* and prioritize its foundational initiatives. IRS agreed with our recommendations and is currently working to finalize its overall authentication approach.

Additional Actions Could Help IRS Enhance Security and Stay Ahead of Fraudsters

Given the widespread availability of personally identifiable information that fraudsters can use to perpetrate tax fraud, it is essential for IRS to further strengthen taxpayer authentication to stay ahead of fraudsters' schemes. In our report, we identified two additional areas that IRS must address to better position the agency and protect taxpayers against future threats.

First, we found that IRS has taken preliminary steps to implement NIST's June 2017 guidance for secure online authentication, however it had not yet established detailed plans, including timelines, milestone dates, and resource needs to fully implement it. Among other things, NIST's new guidance directs agencies to assess the risk for each component of identity assurance—identity proofing, authentication, and federation—rather than conducting a single risk assessment for the entire process.[6] According to NIST officials, this approach gives agencies flexibility in choosing technical solutions; aligns with existing, standards-based market offerings; is modular and cost-effective; and enhances individual privacy. In short, following NIST's new guidance will help provide IRS with better risk-based assurance that the person trying to access IRS's online services is who they claim to be.

As noted in our report, IRS has taken preliminary steps to implement the new NIST guidance. These efforts include forming a task force to guide IRS's implementation of NIST guidance and working with the Security

[6]According to NIST, identity proofing establishes that the person is actually who they claim to be; authentication verifies that the person attempting to access a service is in control of one or more valid authenticators associated with that person's identity; and federation is the concept that one set of user credentials can be used to access multiple systems.

Summit to develop an implementation framework for state and industry partners. IRS has also begun analyzing gaps between IRS's current authentication procedures and the new guidance. In addition, in December 2017, IRS implemented a more secure online authentication option consistent with the new guidance through its mobile application, IRS2Go. After taxpayers link their IRS online account with the mobile app, they can use it to generate a security code to log into their account. This option provides taxpayers with an alternative to receiving the security code via a text message, which NIST considers to be less secure.

We recommended that IRS develop a plan—including a timeline, milestone dates, and resources needed—for implementing changes to its online authentication programs consistent with new NIST guidance, and also implement these improvements. IRS agreed with our recommendations, but noted that its ability to complete these efforts will depend on the availability of resources.

Second, we found that IRS lacks a comprehensive, repeatable process to identify and evaluate potential new authentication technologies and approaches. Our discussions with representatives from industry and financial institutions and with government officials indicate that there is no single, ideal online authentication solution that will solve IRS's challenges related to IDT refund fraud. These representatives advocate an approach to authentication that relies on multiple strategies and sources of information, while giving taxpayers options for further protecting their information.

We identified several authentication options in our report that IRS could consider, including the following:

- **Possession-based authentication.** This type of authentication offers users a convenient, added layer of security when used as a second factor for accessing websites or systems that would otherwise rely on a username and password for single-factor authentication. For example, as noted in our report, according to an industry official, authentication using a trusted device or "security key" based on Universal Second Factor standards complies with NIST's new guidance for digital authentication. While IRS is not likely to provide the devices to taxpayers, it could enable its systems to accept these trusted devices as authenticators for taxpayers who elect to use them.
- **Working with trusted partners.** IRS could partner with organizations it trusts that are accessible to taxpayers and enable the partners to identity-proof and authenticate taxpayers. Trusted partners could

include tax preparers, financial institutions, or other federal or state agencies. In the course of our work, IRS officials stated that they had been exploring such options with both the Social Security Administration and the U.S. Postal Service; however, at the time of our report, the agencies had not yet made decisions about next steps.

- **Expanding existing IRS services to further protect taxpayers.** IRS could expand the functionality of its online account to further protect taxpayers from IDT refund fraud. For example, IRS could develop additional functionality that allows the taxpayer to designate a bank account or a preference for a paper check for receiving a tax refund. If a fraudster filed a return with different information, the return would be automatically rejected.

IRS officials told us the agency continually researches new identity assurance processes and technologies and has talked with other agencies, industry groups, and vendors to better understand how particular technology solutions could apply to IRS's environment. However, during the course of our work, IRS could not provide us evidence of a repeatable, comprehensive process to identify and evaluate available authentication technologies and services. Such a process could compare options for in-house authentication solutions with off-the-shelf solutions based on estimates of cost, schedule, and benefits, as applicable. To this end, we recommended that IRS develop a process to identify and evaluate alternative options for improving taxpayer authentication, including technologies in use by industry, states, or other trusted partners; and based on this approach, include and prioritize these options, as appropriate, in its *Roadmap*. IRS agreed with these recommendations, but did not provide additional details on how it plans to address them.

In conclusion, IRS's authentication environment is one component of a broad, complex information technology infrastructure, and we have previously reported on the many challenges the agency faces as it modernizes its tax systems.[7] Taxpayer authentication has become more difficult with the wide availability of personally identifiable information and fraudsters' ability to develop more complex and sophisticated methods to commit fraud undetected. Addressing the issues we describe above could

[7]We have reported extensively on IRS's IT modernization efforts. See, for example, GAO, *Information Technology: Federal Agencies Need to Address Aging Legacy Systems,* GAO-16-468 (Washington, D.C.: May 25, 2016); and *Information Technology: Management Attention Is Needed to Successfully Modernize Tax Processing Systems,* GAO-18-153T (Washington, D.C.: Oct. 4, 2017).

better position IRS to identify and mitigate vulnerabilities in its authentication efforts and better protect taxpayers and the Treasury.

Chairman Jenkins, Ranking Member Lewis, and members of the Subcommittee, this concludes my prepared remarks. I look forward to answering any questions that you may have at this time.

GAO Contacts and Staff Acknowledgments

If you or your staff have any questions about this testimony, please contact James R. McTigue, Jr. at (202) 512-9110 or mctiguej@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Key contributors to this testimony include Neil Pinney, Assistant Director; Heather A. Collins, Analyst-in-Charge; Dawn Bidne; and Bryan Sakakeeny.