GAO Highlights

Highlights of GAO-18-418, a report to congressional requesters

June 2018

IDENTITY THEFT

IRS Needs to Strengthen Taxpayer Authentication Efforts

Why GAO Did This Study

Strong preventive controls can help IRS defend itself against identity theft refund fraud. These controls include taxpayer authentication—the process by which IRS verifies identities before allowing people access to a resource; sensitive data; or, in some cases, a tax refund. The risk of fraud has increased as more personally identifiable information has become available as a result of, for example, large-scale cyberattacks on various entities. IRS's ability to continuously monitor and improve taxpayer authentication is a critical step in protecting billions of dollars from fraudsters.

GAO was asked to examine IRS's efforts to authenticate taxpayers. This report (1) describes the taxpayer interactions that require authentication and IRS's methods; (2) assesses what IRS is doing to monitor and improve taxpayer authentication; and (3) determines what else, if anything, IRS can do to strengthen taxpayer authentication in the future.

To meet these objectives, GAO reviewed IRS documents and data, evaluated IRS processes against relevant federal internal control standards and guidance, and interviewed IRS officials and state and industry representatives.

What GAO Recommends

GAO is making 11 recommendations to IRS to estimate resources for and prioritize its authentication initiatives, address internal control issues to better monitor authentication, develop a plan to fully implement new NIST guidance, and develop a process to evaluate potential authentication technologies. IRS agreed with GAO's recommendations.

View GAO-18-418. For more information, contact James R. McTigue, Jr. at (202) 512-9110 or mctiguej@gao.gov

What GAO Found

The Internal Revenue Service (IRS) has identified over 100 interactions requiring taxpayer authentication based on potential risks to IRS and individuals. IRS authenticates millions of taxpayers each year via telephone, online, in person, and correspondence to ensure that it is interacting with legitimate taxpayers. IRS's estimated costs to authenticate taxpayers vary by channel.

Taxpayers Authenticated for Selected IRS Programs, 2017

IRS Taxpayer Authentication by Channel

	Telephone Service ☎	Online Service	In-person Service	Correspondence Service ✉
Taxpayers Authenticated	7,211,600	16,502,000	945,100	3,941,700
Estimated Cost Per Interaction	60 cents (automated) to $54 (live assistor)	20 cents	$89	60 cents (mailing) to $65 (document review)

Source: GAO analysis of Internal Revenue Service (IRS) documents and data. | GAO-18-418

Notes: Numbers are rounded to the nearest hundred and represent successful authentications. Cost information is rounded to the nearest dollar unless otherwise noted. Data are for IRS's Taxpayer Protection Program, Get Transcript, Identity Protection Personal Identification Number, and taxpayer online accounts.

IRS has made progress on monitoring and improving authentication, including developing an authentication strategy with high-level strategic efforts. However, it has not prioritized the initiatives supporting its strategy nor identified the resources required to complete them, consistent with program management leading practices. Doing so would help IRS clarify relationships between its authentication efforts and articulate resource needs relative to expected benefits. Further, while IRS regularly assesses risks to and monitors its online authentication applications, it has not established equally rigorous internal controls for its telephone, in-person, and correspondence channels, including mechanisms to collect reliable, useful data to monitor authentication outcomes. As a result, IRS may not identify current or emerging threats to the tax system.

IRS can further strengthen authentication to stay ahead of fraudsters. While IRS has taken preliminary steps to implement National Institute of Standards and Technology's (NIST) new guidance for secure digital authentication, it does not have clear plans and timelines to fully implement it by June 2018, as required by the Office of Management and Budget. As a result, IRS may not be positioned to address its most vulnerable authentication areas in a timely manner. Further, IRS lacks a comprehensive process to evaluate potential new authentication technologies. Industry representatives, financial institutions, and government officials told GAO that the best authentication approach relies on multiple strategies and sources of information, while giving taxpayers options for actively protecting their identity. Evaluating alternatives for taxpayer authentication will help IRS avoid missing opportunities for improving authentication.