May 2019

TAXPAYER INFORMATION

IRS Needs to Improve Oversight of Third-Party Cybersecurity Practices

GAO Highlights

Highlights of GAO-19-340, a report to the Ranking Member, Committee on Ways and Means, House of Representatives

Why GAO Did This Study

Third-party providers, such as paid tax return preparers and tax preparation software providers, greatly impact IRS's administration of the tax system. If these third parties do not properly secure taxpayers' personal and financial information, taxpayers will be vulnerable to identity theft refund fraud and their sensitive personal information will be at risk of unauthorized disclosure. IRS estimates that it paid out at least $110 million in identity theft tax refund fraud during 2017, and at least $1.6 billion in identity theft tax refund fraud during 2016.

GAO was asked to review IRS's efforts to track, monitor, and deter theft of taxpayer information from third parties. Among other things, this report assesses what is known about the taxpayer information security requirements for the systems used by third-party providers, IRS's processes for monitoring compliance with these requirements, and IRS's requirements for third-party security incident reporting.

GAO analyzed IRS's information security requirements, standards, and guidance for third-party providers and compared them to relevant laws, regulations, and leading practices, such as NIST guidance and *Standards for Internal Control in the Federal Government*. GAO reviewed IRS's monitoring procedures and its requirements and processes for third-party reporting of security incidents, and compared them to Internal Control Standards and GAO's *A Framework for Managing Fraud Risk in Federal Programs*. GAO also interviewed IRS and tax industry group officials.

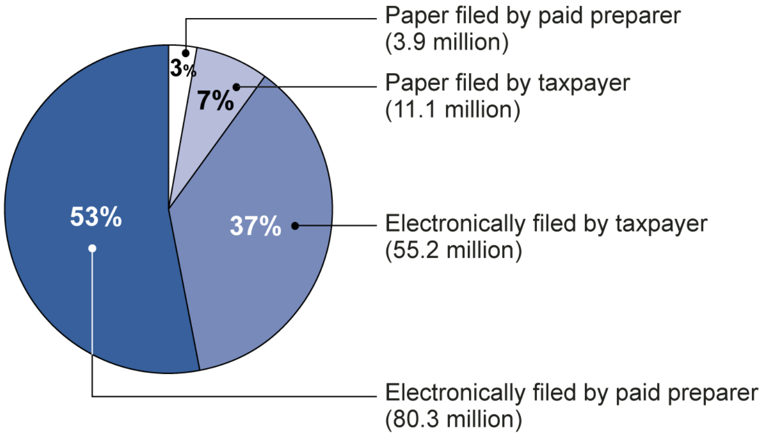
View GAO-19-340. For more information, contact Jessica Lucas-Judy at 202-512-9110 or lucasjudyj@gao.gov

What GAO Found

Federal law and guidance require that the Internal Revenue Service (IRS) protect the confidentiality, integrity, and availability of the sensitive financial and taxpayer information that resides on its systems. However, taxpayer information held by third-party providers—such as paid tax return preparers and tax preparation software providers—generally falls outside of these requirements, according to IRS officials.

In 2018, about 90 percent of individual taxpayers had their tax returns electronically filed by paid preparers or used tax preparation software to prepare and file their own returns.

How Individual Tax Returns Were Filed, Calendar Year 2018



Source: GAO analysis of Internal Revenue Service (IRS) return filing information. I GAO-19-340

IRS seeks to help safeguard electronic tax return filing for various types of third-party providers through requirements under its Authorized e-file Provider program. However, IRS's efforts do not provide assurance that taxpayers' information is being adequately protected.

- Paid Preparers. IRS has not developed minimum information security requirements for the systems used by paid preparers or Authorized e-file Providers. According to IRS's Office of Chief Counsel, IRS does not have the explicit authority to regulate security for these systems. Instead, the Internal Revenue Code gives IRS broad authority to administer and supervise the internal revenue laws. The Department of the Treasury has previously requested additional authority to regulate the competency of all paid preparers; GAO has also suggested that Congress consider granting IRS this authority. Congress has not yet provided such authority. Neither the Department of the Treasury request nor the GAO suggestion included granting IRS authority to regulate the security of paid preparers' systems. Having such authority would enable IRS to establish minimum requirements. Further, having explicit authority to establish security standards for Authorized e-file Providers' systems may help IRS better ensure the protection of taxpayers' information.

What GAO Recommends

GAO suggests that Congress consider providing IRS with explicit authority to establish security requirements for paid preparers' and Authorized e-file Providers' systems.

GAO is also making eight recommendations, including that the Commissioner of Internal Revenue

- Develop a governance structure or other form of centralized leadership to coordinate all aspects of IRS's efforts to protect taxpayer information while at third-party providers.
- Require all tax software providers to adhere to prescribed information security controls.
- Regularly review and update security standards for tax software providers.
- Update IRS's monitoring programs to include basic cybersecurity issues.
- Standardize incident reporting requirements for all types of third-party providers.

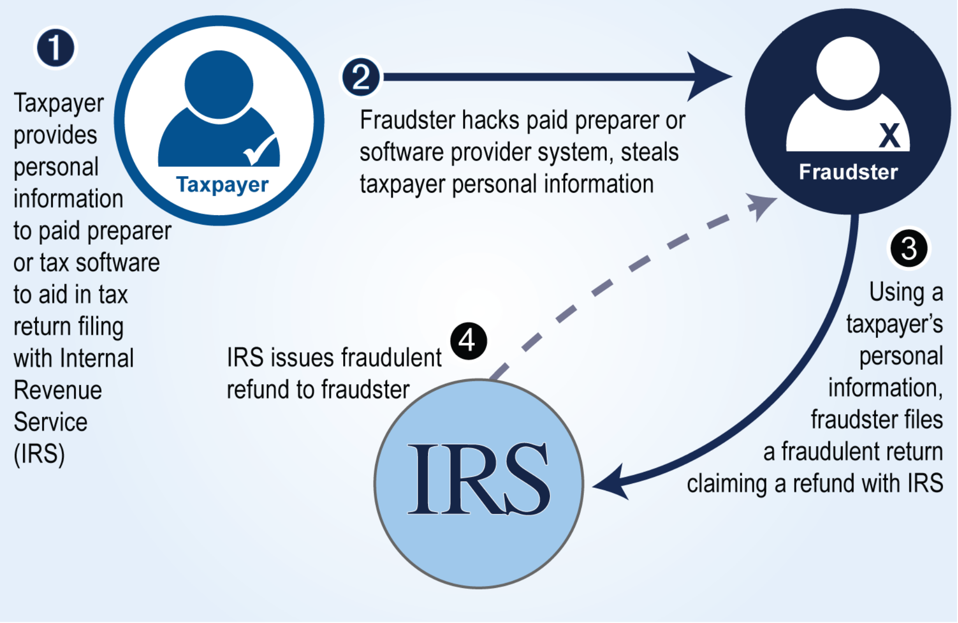
IRS agreed with three recommendations, including the above recommendations to regularly review and update security standards for tax software providers, and standardize incident reporting requirements.

IRS disagreed with five recommendations—including the other three listed above—generally citing the lack of clear and explicit authority it would need to establish security requirements for the information systems of paid preparers and Authorized e-file Providers. GAO believes that IRS can implement these recommendations without additional statutory authority.

- Tax Software Providers. As part of a public-private partnership between IRS and the tax preparation industry, 15 tax software providers voluntarily adhere to a set of about 140 information security controls developed using guidance from the National Institute of Standards and Technology (NIST). However, these controls are not required, and these providers represent only about one-third of all tax software providers. Additionally, IRS established six security, privacy, and business standards for providers of software that allows individuals to prepare their own tax returns (as opposed to software that paid preparers use). However, IRS has not substantially updated these standards since 2010, and they are, at least in part, outdated. For example, IRS cites an outdated encryption standard that NIST recommends not using due to its many known weaknesses.

A key factor contributing to missed opportunities to address third-party cybersecurity is IRS's lack of centralized leadership. Consequently, IRS is less able to ensure that third-party providers adequately protect taxpayers' information, which may result in identity theft refund fraud.

Example of Successful Identity Theft Refund Fraud Attempt


1
Taxpayer provides personal information to paid preparer or tax software to aid in tax return filing with Internal Revenue Service (IRS)
Taxpayer
2
Fraudster hacks paid preparer or software provider system, steals taxpayer personal information
X
Fraudster
3
Using a taxpayer's personal information, fraudster files a fraudulent return claiming a refund with IRS
4
IRS issues fraudulent refund to fraudster
IRS

Source: GAO analysis. | GAO-19-340

IRS monitors compliance with its electronic tax return filing program requirements for those paid preparers who electronically file returns; however, IRS's monitoring has a limited focus on cybersecurity issues. For example, the monitoring techniques largely focus on physical security (e.g., locked filing cabinets) rather than verifying that preparers have an information security policy consistent with NIST-recommended controls. Without effective monitoring of cybersecurity controls, IRS has limited assurance that those paid preparers' systems have adequate controls in place to protect clients' data.

IRS recently began collecting information on high-risk security incidents, such as hackers infiltrating third-party provider systems. Reported incidents increased from 2017 to 2018, the only years for which IRS has data. However, IRS does not have a full picture of the scope of incidents because of inconsistent reporting requirements, including no reporting requirements for paid preparers.

Reported High-Risk Security Incidents at Paid Preparers and Tax Software Providers, 2017 and 2018

	2017	2018
Number of security incidents	212	336
Number of taxpayer accounts affected	180,557	211,162

GAO analysis of Internal Revenue Service data. | GAO-19-340