Thieves targeted $12 billion through IRS tax fraud

Joe Davidson
The Washington Post, October 19

The Internal Revenue Service building in Washington. Two government watchdogs say the IRS should do more to stop online tax fraud. (Susan Walsh/AP)

Like others in business, thieves know a fertile market when they see it.

As sophisticated cybercrooks look at the Internal Revenue Service (IRS), and the $383 billion it paid out in fiscal 2017, their eyes must glaze with dollar signs.

The IRS estimated online robbers attempted to steal least $12.2 billion, if not more, through identity theft tax refund fraud in 2016, according to the Government Accountability Office (GAO). IRS vigilance thwarted most of those attempts, but the fakers got away with at least $1.6 billion. The good news is the 2016 data represent a steady and significant drop in tax identity theft since 2012.

Taxpayer protections are strong, but not strong enough, according to reports from two government watchdogs. There are holes in the electronic fence protecting taxpayer data, gaps the agency must move quickly to fix.

When GAO and Treasury Inspector General for Tax Administration (TIGTA) officials describe IRS efforts to improve taxpayer security, they repeatedly qualify with “however.”

“For example, the IRS deployed a more rigorous electronic authentication process that provides two-factor authentication via a security code sent to text-enabled mobile phones,” Michael E. McKenney, a deputy inspector general, told a recent House Ways and Means oversight subcommittee hearing. “However, these improvements only applied to five online applications.” That’s just 10 percent of the agency’s 52 electronic portals available for taxpayers to share information with the agency.

James R. McTigue Jr., GAO’s strategic issues director, acknowledged “IRS has taken some steps to improve taxpayer authentication.”

Then he said, “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” security guidance from the National Institute of Standards and Technology (NIST).

With increasing reliance on computerized transactions in every sphere of life comes ever-growing ways for burglars to steal from us, without being anywhere near us. The 52 online applications are like 52 doors to a house. The doors have locks, but they aren’t strong enough to keep all the thieves out.

“For example, in May 2015, the IRS discovered that criminals used taxpayers’ personal identification information obtained from sources outside the IRS to impersonate the taxpayers and gain unauthorized access to tax information in its Get Transcript application,” McKenney said. “TIGTA believes that the system was widely exploited by numerous bad actors who collectively made at least 724,000 potentially unauthorized accesses to taxpayer accounts, resulting in the filing of 252,400 potentially fraudulent tax returns and the issuance of $490 million in potentially fraudulent refunds.”

IRS officials know cases like those must be stopped.

“Protecting taxpayers and their data is not just the job of our offices, it is a foundational priority across the IRS, and an extremely important aspect of taxpayer service,” said Edward Killen, the agency’s chief privacy officer. “Our systems currently withstand an average of 2.5 million intrusion attempts daily."

From 2015 to 2017, he said, “the number of taxpayers reporting to the IRS that they were victims of identity theft dropped by 65 percent, and the number of tax returns with confirmed identity theft fell by 57 percent with more than $20 billion in taxpayer refunds being protected.”

Feeding tax fraud are data breaches not connected to the IRS. McKenney cited the 500 million Yahoo customers, the 145 million who have records with Equifax and the 21.5 million people with Office of Personnel Management files whose personally

identifiable information, such as birth dates and Social Security numbers, might have been breached in cyberattacks.

“Recent cyber events against the IRS have illustrated that bad actors are continually seeking new ways to attack and exploit IRS computer systems and processes in order to access tax information for the purposes of identity theft and filing fraudulent claims for tax refunds,” McKenney said.

Among the “bad actors”:

♦Thirty-three people pleaded guilty to claiming $22 million through fraudulent tax returns using “other individuals’ personal identification information — obtained in part from patients and employees of the Battle Creek Veterans Affairs Medical Center and from inmates of the Michigan Department of Corrections,” according to a January 2017 news release from the U.S. attorney’s office in Grand Rapids, Mich.

♦Anthony and Sonia Alika were sentenced in 2016 for their roles in a fraud involving “cyber intrusions, identity theft, phony tax returns and money laundering, all to the order of millions of dollars,” according to the Justice Department office in Atlanta. Anthony Alika and Rapheal Atebefia also used the names and Social Security numbers of others to access the IRS’s “Get Transcript” database to file phony tax returns.

♦Abdulrahman Tijani, along with others in another Get Transcript case, filed 47 bogus tax returns, seeking $265,960 in refunds, during a seven-week period in 2015 using stolen personally identifiable information, according to department officials in Atlanta. The IRS suspected 35 were potentially fraudulent. The department’s criminal complaint linked the scheme to the Get Transcript scam that McKenney mentioned. Tijani, 41, of Lawrenceville, Ga., was ordered in August to pay $50,221 in restitution and sentenced to four years in prison. After that, he’ll probably be deported.

Inspector General J. Russell George said, “Let this case serve as a warning to others who are interested in exploiting the Internal Revenue Service’s computer systems to commit identity theft and other forms of criminal activity.”

It’s a warning many will not heed.

Read more:

Thieves stole taxpayer data from IRS ‘Get Transcript’ service

Private tax collection, raising much less than expected, hit again

Will scammers hide behind new law for private tax collectors?

Private tax collection agencies lose money while going after the poor