IRS warns tax preparers about a new refund scam

Only a few days into the tax-filing season, the IRS is sounding an alarm about a new tax scam. Specifically, it's warning tax preparers to be on guard about the scam, which is aimed at stealing taxpayers' refunds by using data compromised in tax preparers' offices.

The agency said it has already received a number of fake tax returns that had accurate taxpayer names, addresses, Social Security numbers and even bank account information for the victims.

In an unusual twist, some bogus refunds were actually directed to the real taxpayers' bank accounts, the agency said. A criminal, posing as a debt collector, then contacted the taxpayers saying the refunds had been sent in error and the victims should forward the money to the crook.

Because these fake returns contained all of the taxpayer's correct information, down to the right number of dependents, the IRS believes the scam started in tax-preparation offices. The agency assumes that the data was compromised because some preparers were taken in by phishing scams that then loaded malicious software onto their computer systems, making all the taxpayer information that was kept by these preparers vulnerable to theft.

Government website to help victims of identify theft

The IRS said it's still in preliminary stages of investigating the con and can't quantify how many people have been affected. But because this type of scam has a way of burgeoning overnight, the agency wanted to immediately warn preparers to secure their computer systems.

"Given the history that we have seen on scams like this, when these start, they tend to proliferate quickly," said IRS spokesman Terry Lemons. "When a scam turns out to be successful, they tend to expand. We wanted to alert tax professionals to be on the lookout."

Unfortunately for consumers -- the ultimate victims of this con -- those who find themselves hit by tax fraud have a far more difficult course than consumers whose credit card accounts have been stolen. In the latter case, consumers have a number of steps they can take to deter criminals from using that stolen information to open up new accounts.

In the former case, the first inkling that a taxpayer would get that they were victimized is when their electronically filed return gets rejected as a duplicate. At that point, in addition to reporting the fraud to the credit bureaus and the Federal Trade Commission, tax fraud victims need to fill out a special IRS form, 14039. The taxpayer's 1040 must then be filed on paper, with the fraud affidavit attached to the front.

How the tax bill will affect the returns of three American families

Be prepared that this will dramatically slow your refund. Lemons said the typical tax identity fraud takes roughly four months to investigate and resolve.

Since tax ID theft peaked in 2013, the IRS has taken a host of steps, including forming a security partnership with preparers and software companies, to stamp out tax return fraud. The agency has also launched a pilot program that has added 16-digit identifiers to some employer's W-2 information. The agency hopes this will help it spot and stop identity thieves before they take off with taxpayer refunds.

These efforts have helped cut ID theft reports nearly in half over the past year.

"We have stepped up our defenses, and the private sector tax community has worked to strengthen their security too," Lemons said.

Still, this newly discovered fraud is ominous and suggests that individual taxpayers should also be on guard.

Make sure that you keep updated security software on your home computer and ask any tax preparer you hire how your data is protected, Lemons suggested. If any of your W-2 forms contain the new 16-digit identifiers, also make sure to include that number on your tax return. That will help the IRS know the return truly came from you, not an identity crook.

By Kathy Krisof