want to find out is what specific information was compromised. But, until recently, the IRS has had a policy in place that prevented identity theft victims from ...

Jul. 22, 2015

If you have ever had a client facing identity theft, you know that the first thing they want to find out is what specific information was compromised. But, until recently, the IRS has had a policy in place that prevented identity theft victims from having access to the fraudulent returns filed in under their names. Thankfully, due to the efforts of New Hampshire Senator Kelly Ayotte, the IRS approach to disclosure of information on fraudulent tax returns is changing.

While the procedure has not been finalized, the IRS announced on May 28th that it will change its policy for disclosing identity theft tax returns to those under whose names and social security numbers the tax returns were filed. Upon request, tax identity theft victims soon will be able to obtain redacted copies of the tax returns submitted under their social security numbers.

Tax identity theft has been an evolving problem and a growing concern for several years, with the number of reported incidents doubling from one to two million from 2011 to 2013. As of June of this year, the IRS reportedly had blocked three million fraudulent 2014 tax filings.

Under the realization that identity theft is a major threat showing no signs of going away, this year IRS Commissioner Koskinen held a Security Summit Meeting with state tax administrators and CEOs from leading tax and financial software companies to identify solutions for detecting and preventing identity theft and fraud. The set of solutions recommended and agreed upon includes pre-refund authentication via identity theft fraud detecting filters and algorithms, post-filing

analytics, information sharing, identity-proofing, and initiatives to raise taxpayer

direction, it remains a major threat. With the ever-increasing sophistication of hackers, there is often little we can do to protect our clients from becoming ID theft victims on the Internet. But there is quite a bit we can do in our own offices. Here are some tips for ensuring proper handling of your clients' personal identifying information and keeping it safe:

- Do not send or receive your clients' tax returns through email; share information through a secure portal or document sharing website only.
- Do not release client information to third parties unless you are required to by law or court order.
- If you have employees and/or vendors, set up and maintain internal controls over access to information. Grant access only on an as-needed basis.
- Avoid travelling with physical documents; instead, keep sensitive information stored on an encrypted hard drive and/or a secure website.
- Require strong passwords to access all computers and devices storing sensitive data, and don't leave the password on a piece of paper taped to the monitor. Change the password on a regular basis.
- Keep up-to-date and continuously monitoring antivirus software on your computer.

Many of the new information validating protocols arising from the March Security Summit meeting are expected to be in place by the time the 2016 filing season hits. In the meantime, consider the above tips while making awareness of identity theft a routine part of the discussions you have with your clients.

———

Dave Du Val, EA, is VP of Customer Advocacy at TaxAudit.com, an IRS audit defense service.

Sponsors.