PRODUCT & SERVICE GUIDE

Tax Identity Theft and Your Clients: 5 Steps to Finding Peace

With the Equifax data breach exposing the personal identifiable information (PII) of 143 million Americans this year, we will need to be prepared to receive and answer more concerns than ever from our clients about tax related identify theft this ...

Dave DuVal, EA • Nov. 28, 2017

If Your Clients Are Worried About Tax Identity Theft

With the Equifax data breach exposing the personal identifiable information (PII) of 143 million Americans this year, we will need to be prepared to receive and answer more concerns than ever from our clients about tax related identify theft this coming tax season.

But while the IRS has been steadily improving safeguards against tax identity theft every year, there is still very little an individual – or their tax professional – can do to prevent tax identity theft once their information has been compromised. The best strategy for any taxpayer remains the same: file your return as early as possible in order to beat the identify thieves to the punch. That said, there are a few things we can do to help our clients who may be worried.

Set Expectations

We can help our clients by setting expectations for a tax season that may be fraught with delays. Filing early is an excellent proactive measure, but it may not prevent a refund from being held up. With heightened security around identity theft, any of

our clients may find their refunds withheld indefinitely with little explanation from the IRS.

In addition, we may find it necessary to help our clients understand the limits of their control over tax return identity theft. For example, it might help to alert our clients that putting credit freezes on their credit accounts after being notified that their information was compromised may help prevent credit card fraud, but it is unlikely to prevent tax return fraud; a credit freeze does nothing to stop an identity thief who has enough of a client's personal identifiable information from filing a fraudulent tax return in their names.

Though state definitions may differ slightly, personal identifiable information (PII) is any data that could potentially identify a specific individual. PII generally includes any of the following: an individual's name, date of birth, credit card numbers, social security number, financial records, credit report date, state identification or driver's license number, telephone numbers, addresses, names of relatives, photographs, or anything else that can be used to identify an individual.

Be Proactive

We can help our clients be proactive against potential tax identity theft by giving them a little nudge just after the New Year. We can call them in early January to review their prior year's return and discuss the information documents and receipts for potentially deductible expenses they will need to complete their returns for the current tax year – and ask to set up their tax appointments for the earliest possible time, while letting them know about our concerns for the upcoming filing season.

A client who has already been a victim of identity theft tax fraud may be eligible for an Identity Protection Personal Identification Number (IP PIN). An IP PIN is an assigned number that is used when filing to authenticate the tax filer's identity. Any client whose Social Security number has been compromised and who has been informed by the IRS of a possible identity theft tax fraud, or whose e-filed return is rejected as a duplicate, should complete and file Form 14030, Identity Theft Affidavit. In addition, clients who filed a tax return last year in Georgia, Florida, or Washington D.C. are able to obtain an IP PIN.

Monitor

Once our clients file their returns, they may want to set up an account with the IRS that allows them to monitor the details of their tax activity. While it can be a bit of a

hassle to set up, being able to check in on the activity might provide them with the extra peace of mind they need if they are concerned.

Be Positive

Despite the additional worry caused by the data breach, there is quite a bit to be hopeful about that we can share with our clients. The IRS and its Security Summit Partners have been making steady progress over the past several years in combatting tax identity theft. The number of identity theft returns has been declining since 2015, and the number of people who are reporting themselves to be identify theft victims has also been declining substantially.

The tax industry has been sharing data points that have helped the IRS and states identify potential identity theft fraud – and this year they will be sharing more data points than they have in past years, which should help to further reduce tax related fraud. Additionally, the IRS and Security Summit Partners are continuing to share information about emerging identity theft schemes in the Identity Theft Tax Refund Fraud information and Sharing and Analysis Center.

While the Equifax breach may have exposed enough PII for someone to file a fake return, new protections are in place that may prevent them if they try. The IRS and Security Summit Partners from the federal, state, and private sectors are further refining the existing tax return security protections for the 2018 tax season. For example, beginning in 2018, 66 million W-2 forms will include a new "Verification Code" box (Box 9 of the W-2 Form) that will authenticate their W-2 as they file their tax return.

Be Vigilant

Even with the incredible progress being made to combat identity theft, keeping W-2 and other financial data secure remains critical – especially for our clients whose PII has been compromised. The holiday season is a great time not only for end of year tax planning, but also to remind our clients of the need for vigilance in keeping their information secure. This includes never sending confidential documents containing PII to anyone via email, ensuring documents are stored in a secure location, shredding documents before disposing of them, maintaining firewalls, practicing safe web browsing, using best practices for password creation, and understanding how to identify and avoid social engineering schemes.

Data breaches are beyond our control. Once an identity thief gets hold of our clients' personal information, there is little we can do to prevent tax identity theft from happening to them. But we can still help by encouraging our clients to file as early as possible, monitor the activity in their accounts, and to be vigilant about their information and cyber security in order to minimize any resulting damage from compromised personal data.

———

Dave Du Va is an Enrolled Agent and the Chief Customer Advocacy Officer for TaxAudit and Audit Defense Pro. At TaxAudit, he ensures that the entire team is on the forefront of tax education, research, best practices, and audit representation. At Audit Defense Pro, Dave focuses on making sure the staff has the knowledge and technical experience to provide quality audit representation.

He is an Enrolled Agent and federally authorized tax practitioner, who has prepared thousands of returns during his career and has trained and mentored hundreds of tax professionals. He is a member of the National Association of Tax Professionals, the National Association of Enrolled Agents, and the California Society of Enrolled Agents. He is a frequent guest speaker for the California Society of Tax Consultants, the California Society of Enrolled Agents, and the National Association of Tax Professionals.

Product & Service Guide • Tax • Article • Data Breach • identity theft • identity theif

CPAPA is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.