Financial and Tax-Related Identity Theft

The new frontier of fraud

By Blake Christian, CPA/MBT

Key Takeaways:

- A recent AICPA survey showed that over one-third of older adults and 22 percent of millennials fell victim to identity theft last year.
- With the combination of billions of e-documents, server and cloud-based databases, and sophisticated hackers, this trend will likely get much worse in the short term.
- You should take precautions now to protect your personal information and should enroll in credit monitoring services as a preventive measure. Most services are free or minimal cost.

With last year's revelation that the IRS data breach involved over 330,000 taxpayer records (the IRS originally reported only 104,000 records were compromised), and more breaches were just announced, the IRS is finally under sufficient pressure to implement some formal procedures to assist taxpayers who have experienced a governmental, corporate or other data breach.

Due to the massive credit card breaches at various financial institutions—Target, Home Depot and other retailers; attacks on government agencies; and the most recent web fiasco, Ashley Madison—identity theft is now the most common consumer complaint, with over 10 million total identity theft cases per year and rapid growth every year.

It is important to know how to act if you ever fall victim to identity theft. If nothing else, make sure your financial advisors are kept in the loop and are familiar with the various schemes, preventive measures and corrective actions.

Identity theft is clearly a growing trend with very serious repercussions for consumers, web designers and webmasters, taxpayers, businesses, and government agencies. For taxpayers, a data breach can result in loss of funds, delayed tax refunds, cloned identities and/or damaged credit ratings—not to mention a massive time drain to sort out the extent of the thieves' activities. And organizations that did not prevent the breach can face expensive lawsuits, loss of consumer trust and decreased revenue for retailers and other businesses. That's an issue, even for those of you who own smaller businesses.

For one dollar, you can enroll in Experian's credit monitoring service and review your current credit standing on all three credit bureaus: www.creditchecktotal.com. Enrollment and a review of your open credit accounts and personal data take less than 10 minutes and will give you a very good picture of whether or not you have been breached. If you suspect that your data has been breached (e.g., you see new credit card accounts that you did not open, or personal information has been altered), you should immediately contact all three major credit bureaus (Equifax, Experian and TransUnion) and alert them to the possibility of fraud. The next organizations to notify are the IRS and state tax authorities, since your tax accounts are also prime targets for hackers.

While all breaches are serious, the IRS breaches are some of the most worrisome, since the IRS houses hundreds of millions of highly confidential records (including Social Security numbers for all family members), which are a treasure trove for these sophisticated hackers. The thieves might also get access to taxpayers' IRS account information from other data breaches discussed above.

Here are some precautions you can take to prevent identity theft cases:

- Enrolling in various credit monitoring services. Note that most people can get free credit monitoring services as a result of being a customer of Anthem, Target, Home Depot, or other retailers or financial institutions that experienced a credit card database breach.
- Shredding any unneeded personal files at home and at work.
- Protecting Social Security numbers on the web, over the phone and in letters, etc. Generally including the last four digits is fine for existing accounts.
- Preventing personal financial information from being shared over the phone unless you are positive who the other party is. A good rule of thumb for incoming calls associated with any accounts is to get the caller's number, check the number out and return the call if it looks legitimate.
- Do not use public Wi-Fi networks when dealing with banking, investment and tax data. Use a secured virtual private network (VPN) and encrypt emails if personal information must be sent via the Internet.
- Obtain or review your umbrella insurance policy to determine whether the insurance company will cover costs to repair your credit and for problems caused by identity theft.

Conclusion

Accessing any one of the many IRS systems or databases can be the Holy Grail of data for tech criminals. Access to taxpayers' and dependents' Social Security numbers, home and business addresses, and income sources can spell disaster for the victimized taxpayers whose records have been compromised—and can now be cloned. In Part 2 of this article, we'll look more closely at identity theft issues affecting taxpayers and the IRS and specific actions to take after your data has been breached.

About the Author

Blake Christian, CPA/ MBT *is a Tax Partner in the Park City and Long Beach offices of California-based Top 50 CPA firm HCVT LLP. Blake has over three decades of experience and specializes in corporate and high net-worth individual income, estate and gift tax planning. Blake is a frequent speaker and author and is a thought leader in best practices for professional service firms.*