IDENTITY THEFT: THE TAX AND FINANCIAL IMPLICATIONS

LAURA E. LAFORGIA, CPA, MST

JUNE 2013

Marks Paneth & Shron LLP
Certified Public Accountants & Consultants

IDENTITY THEFT: THE TAX AND FINANCIAL IMPLICATIONS

By now, everyone is familiar with the phrase “identity theft” and probably knows someone who has been hurt in some way from it. Identity theft occurs when someone uses your personally identifying information, such as your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes. The Federal Trade Commission (FTC) estimates that as many as 10 million Americans have their identities stolen each year. Identity theft can be especially devastating when it comes to tax and finances, and it’s essential for CPAs to learn the basics of how to avoid it, spot it and fix the situation after it's happened.

The FTC states on its website that identity theft “can wreak havoc with your finances, credit history, and reputation— and can take time, money, and patience to resolve.” Most people, however, overlook the ways that their personal information is vulnerable to the eyes of criminals. It is not merely an issue anymore of someone rummaging through your trash or stealing your mail (although that is quite common). Criminals have kept up with technology to continually find new ways to steal your personally identifying information. Unfortunately, society has not kept up with criminals in blocking their schemes. Here are just a few of the vulnerable areas:

- Interview questionnaires
- Credit and background checks
- Medical and dental files
- Online activities
- Tax and financial documents
- Poor computer security

The following are the kinds of techniques thieves can use to steal identities, and tips to help you avoid them:

- Skimming – using a device to read a credit card's magnetic strip. A handheld device used as a retail outlet to make purchases, or a device placed over the normal card reader of an ATM, can steal your data when you try to withdraw money. Tip: Keep your eye on your credit card at all times. In addition, if an ATM or store terminal looks funny, don't use it.
- Phishing – emails or phone calls designed to look like official messages from companies that ask you to update your account information. Tip: Think *first*, click *second*. Who is this company or agency requesting information? The email may say "state tax department" but do the links actually go there? Generally, government agencies do not request sensitive information via email.
- Changing your address without your knowledge – your mail, along with your personal information, is redirected to the thief's location. Tip: Pay attention to the mailing cycle of your bills.
- Stealing your records from companies’ storage.
- Pretexting – pretending to be you or someone else with the intention of obtaining your personal information. (A recent well known pretexting case involves a woman arrested for pretending to be a relative of a child killed in the Newtown school shooting with the intention to scam donors.)

This is just the beginning. Fortunately, there is a wealth of free resources available to the public. You can find helpful information on the FTC website. The IRS has a toll-free line specific to this issue (800-908-4490). You can also find good information from the IRS as

well as the Social Security Administration (SSA). Both the IRS and SSA have written publications on this topic: IRS Publication 4535, *Identity Theft Prevention and Victim Assistance,* and SSA Publication No. 05-10064ICN, *Identity Theft and Your Social Security Number.*

Identity Theft Emergency Response

As soon as you suspect identity theft, you need to act very quickly. Immediate action not only stops a thief from doing more damage but it may shorten the amount of time it takes you to clean it up. Accountants can not only use the information in the following paragraphs to help themselves, but they can assist clients by working with the relevant government agencies. In such instances, it's often necessary for clients to fill out and sign "power of attorney" forms.

Call your bank and credit card companies to alert them of your suspicions. If there has been fraudulent activity on your account, you will be required to complete an affidavit of fraud and submit documentation.

Contact the fraud department of all three credit bureaus to place an initial fraud alert on your credit reports, which is good for 90 days. While the first credit bureau you contact is responsible for notifying the other two, you want to be certain. In some cases your credit card company will have already called the credit bureaus, but you should always confirm. You will also receive a case number. The three credit bureaus and their contact numbers are:

- Equifax (800-525-6285)
- Experian (888-397-3742)
- Trans Union (800-680-7289)

File a complaint with FTC, either online or by phone, at (877-438-4338). You will receive a reference number.

Once the identity theft has been confirmed, file a report with local or state police. You will need the police report to place an extended seven-year credit alert on your file.

If there is indication that your driver's license is being misused, contact your state's department of motor vehicles (DMV) to complete a fraud report form. In New York, this form is DMV Form FI-17. You must have evidence of fraud to complete this form.

Long-Term Damage Control

Good recordkeeping is very important during this long process of cleaning up the damage. The easiest way to stay organized and have everything ready for fast access is to keep an organized binder with dividers. The front of the binder should contain a daily log of all activity such as phone calls, emails sent and letters mailed, along with case and reference numbers. Other sections of the binder will include your credit reports, correspondences, and any evidence you gather.

The fraud alert of your account will slow down the perpetrators until they eventually move on. Be patient with the process. It is recommended that you sign up with a credit card service to watch your credit account. You will then be able to log on and review your records for unusual activity. In the beginning of the ordeal, you will want to do this at least

daily. Sign up for alerts (delivered via text or email) from the service to notify you when someone has viewed your credit. (Companies do need your permission, but some may find a way to do this illegally without permission.) This is far more advantageous than waiting for new accounts to appear on your report.

Remember, it is to your advantage to act quickly. It could take as long as two weeks for a new account to show up on your credit report; however, if someone "views" your credit, it will show up within two days. Note that your normal creditors will periodically review your credit and you will get these "good" alerts as well—don't panic every time you receive an alert. If, however, you are not familiar with the company viewing your credit, it is worth a phone call to the company.

You can obtain valuable information for your case by monitoring changes on your credit report. For example, after my identity was stolen and my credit had a fraud alert issued, the perpetrator did not give up easily. The perpetrator kept trying to open accounts and file tax returns even after the alert was issued. One daily alert indicated that a particular bank had viewed my credit. I called the bank and asked why they were looking at my credit. They notified me that they did the financing for a motorcycle shop that I had bought a motorcycle from the day before. I called the shop and explained the situation to the manager. I was able to get a description of the impostor, the ID that she used, as well as exactly what information she knew about me, such as employment. Had I waited, I may not have received such clear information from him. Note that even though I had a fraud alert on my account, the perpetrator still walked away with a motorcycle while the loan was being processed. The shop had poor internal controls in place and learned a valuable lesson.

What Are Your Rights as an Identity Theft Victim?

You are not without recourse in the battle against identity theft. As the victim, you have the following rights:

- To place a 90-day initial fraud alert on your credit report.
- To place a seven-year extended fraud alert on your credit report.
- To receive a free credit report from each of the three credit reporting companies.
- To dispute fraudulent information.
- To ask credit reporting companies and businesses to block erroneous information you are disputing from appearing on your credit report.
- To get copies of documents used by the thief.
- To stop calls and letters from debt collectors.
- To obtain an identity protection personal identification number (IP PIN) from the IRS to use on their returns.

Everyone is entitled to receive a free credit report once a year from each of the three credit reporting agencies. To get your free credit report, go to annualcreditreport.gov or call (877-322-8228). Do not contact each credit agency separately—this is the *official* website to get the legally mandated free credit report, and you will be asked several questions to verify your identity. Be wary of using any other website to order free credit reports as many sites have strings attached to the "free." Unfortunately, this website is a bit confusing to navigate, so be patient.

Tax Identity Theft

As the e-file mandate phased in the last few years, tax identity theft exploded. While electronic filing increases efficiencies of processing tax returns and issuing refunds, it allows criminals to benefit from gaping holes in electronic security. It is fairly easy for a criminal to obtain a real name and social security number, and file an income tax return with a fake W-2 or business income schedule with intent to obtain a fraudulent refund that is deposited right into the criminal's bank account. Additionally, if the victim happened to pay estimated tax payments during the year that the criminal "forgot" to include, the IRS or state agency will be happy to point out the error and refund those payments to the criminal as well. While you will not be held accountable for fraudulent actions of others, it creates a time-consuming mess for you to clean up.

If you have been the victim of tax identity theft, contact the IRS. An agent will put you in touch with the IRS Criminal Investigation Division which detects and investigates tax fraud and other financial fraud, including fraud related to identity theft. In addition, you will be asked to file IRS Form 14039, *Identity Theft Affidavit.*

After a scolding report from the U.S. Government Accountability Office in late 2012, the IRS has expanded, and will continue to expand, their identity theft efforts. They currently have more than 3,000 employees who work on identity theft cases. They are also working on internal controls to decrease the number of days it takes to resolve cases. For 2013, the IRS's expanded efforts include:

- Improving screening filters that spot fraudulent returns before refunds are issued.
- Adding additional IRS criminal investigations.
- Expanding a pilot program that allows state and local law enforcement agencies in 50 states to obtain tax return data from the IRS, with the victim's permission, and assist in investigations.
- Collaborating with more than 130 financial institutions to identify fraud schemes and block fraudulent refunds.
- Permanent Allowance of Truncated Taxpayer Identification Numbers on some individuals' payee documents.

The IRS will now issue an IP PIN for identity theft victims, as well as those who could be exposed to identity theft. The IRS flags your account and uses the IP PIN to make sure your return isn't being fraudulently filed. Unfortunately, even with this new system, your refund will still be held up for several months as the IRS sorts all the information out. The IP PIN is only good for one year and a new one will be issued each year for as long as the account is flagged. Your IP PIN should obviously be kept private. In addition, if you need to file an extension, you will have to paper-file the extension.

Earlier this year, New York State tax department updated its guidance on identity theft. It posted a clear outline on its website on what to do in the event you are affected. For example, if you are an actual victim, or suspect that you are a potential victim, the NYS tax department advises you to complete Form DTF-275, *Identity Theft Declaration* and submit it with copies of your government issued ID, proof of address, a statement explaining why you believe you are a victim of identity theft, and any notice you may have received from NYS.

Other Agencies United

Cybercrime is one of the fastest growing areas of crime, which can include identity theft activities. The Internet Crime Complaint Center (IC3), is a multi-agency task force comprised of the Federal Bureau of Investigation, the National White Collar Crime Center, and the Bureau of Justice Assistance. The IC3 serves as a central hub, offering victims convenient and easy access for reporting complaints of internet crime and refers them to the appropriate law enforcement agencies. Note that filing a complaint with IC3 does not serve as notification to your credit card company that you are disputing unauthorized charges—think of this task force not as assisting in clean-up, but as assisting in catching the crooks. They also indicate on their website: "The confidentiality of the information you provide may be affected by state law. As such, we cannot guarantee that your complaint will remain confidential."

On April 10, 2013, the Commodity Futures Trading Commission (CFTC) and the SEC jointly issued final rules and guidelines that expand and clarify the SEC and CFTC's responsibility regarding oversight and enforcement of identity theft rules. These final rules, which become effective May 20, 2013, require certain investment advisors and regulated entities to establish programs to address risks of identity theft. These provisions were born out of the Dodd-Frank Wall Street Reform. The importance of these rules can't be overlooked. Entities that fall under these rules must implement procedures to detect and respond to identity theft red flags, as well as train staff on identity theft policies and procedures. This will help keep your tax and financial records from the eyes of identity thieves.

As technology has advanced over the last several years, identity theft has grown at an alarming rate. Identity theft will continue to grow unless we keep ahead of the thieves and continually modify and expand identity theft prevention controls. While the IRS has taken steps to improve efforts to fight tax-related identity thefts, it must continually review and expand its policies in place, to keep up with advancing technology.

This article was originally published in *Tax Stringer,* a publication of the New York State Society of CPAs (NYSSCPA), June 2013.

About Laura LaForgia

Laura E. LaForgia, CPA, MST, is a partner at Marks Paneth & Shron LLP, specializing in tax issues related to high net worth individuals and family groups, as well as estates, trusts and private foundations. She is a longtime member of the NYSSCPA Trust and Estate Administration Committee, and is also a member of the National Association of Female Executives and the Estate Planning Council of New York City. In addition to her professional activities, she volunteers her time with animal rescue groups. She can be reached at 212-710-6214.

Contact Laura LaForgia:
Phone: (212) 710-6214; Fax: (212) 710-6215
llaforgia@markspaneth.com

About Marks Paneth & Shron LLP

Marks Paneth & Shron LLP is an accounting firm with over 500 people, of whom nearly 65 are partners and principals. The firm provides public and private businesses with a full range of auditing, accounting, tax, consulting, bankruptcy and restructuring services as well as litigation and corporate financial advisory services to domestic and international clients. The firm also specializes in providing tax advisory and consulting for high-net-worth individuals and their families, as well as a wide range of services for international, real estate, media, entertainment, nonprofit, professional and financial services, and energy clients. The firm has a strong track record supporting emerging growth companies, entrepreneurs, business owners and investors as they navigate the business life cycle.

The firm's subsidiary, Tailored Technologies, LLC, provides information technology consulting services. In addition, its membership in Morison International, a leading international association for independent business advisers, financial consulting and accounting firms, facilitates service delivery to clients throughout the United States and around the world. Marks Paneth & Shron LLP, whose origins date back to 1907, is the 34th largest accounting firm in the nation and the 16th largest in the New York area. In addition, readers of the New York Law Journal rank MP&S as one of the area's top forensic accounting firms for the third year in a row.

Its headquarters are in Manhattan. Additional offices are in Westchester, Long Island and the Cayman Islands. For more information, please visit www.markspaneth.com.