What to Do About Tax-Related Identity Theft

Although most of the public is well aware of how prevalent tax-related identity theft is, the statistics are startling. According to the IRS Taxpayer Advocate Service, tax-related identity theft has risen more than 650% between 2008 and 2012. As stated in a recent *Wall Street Journal* article, the IRS paid out more than $39 million in fraudulent refunds for 2014.

It is increasingly difficult to protect our personal information in today's electronic world. Most of us write checks online (which may actually be safer than the old way). We receive bills and statements online. We use debit and credit cards. We join Facebook to enjoy the news and photos from family and friends. Tax returns are filed electronically. Our identity is everywhere.

The IRS has more than 3,000 employees working on identity-theft cases – more than twice the level of a year ago. They have trained more than 35,000 employees who work with taxpayers to recognize and provide assistance when identity theft occurs. Consumers may find themselves looking for help if this happens to them. On their website, the IRS recommends taking the following steps to help prevent this type of fraud:

- Don't routinely carry your Social Security card or any document with your Social Security Number (SSN) on it.
- Don't give a business your SSN just because they ask – only when absolutely necessary.
- Protect your personal financial information at home and on your computer.
- Check your credit report annually.
- Check your Social Security Administration earnings statement annually.
- Protect your personal computers by using firewalls and anti-spam/anti-virus software. Update security patches and frequently change passwords for internet accounts.
- Don't give personal information over the phone, through the mail, or over the internet, unless you have either initiated the contact or are sure you know who is asking.

RESOURCE CONSULTING GROUP
Integrated Wealth Management Since 1988
301 East Pine Street | Suite 600 | PO Box 4930 | Orlando, FL 32802-4930
(407) 422-0252 | (800) 448-0252 | Fax (407) 649-8795 | www.resourceconsulting.com

Should you become a victim, here are the steps the IRS recommends taking:

- File a report with law enforcement.
- File a complaint with the Federal Trade Commission (FTC) at www.identitytheft.gov or the FTC Identity Theft Hotline at 1-877-438-4338 or TTY 1-866-653-4261.
- Contact one of the three major credit bureaus to place a 'fraud alert' on your credit records:
  - Equifax - www.Equifax.com or 1-800-525-6285
  - Experian - www.Experian.com or 1-888-397-3742
  - TransUnion - www.TransUnion.com or 1-800-680-7289
- Contact your financial institutions; close any accounts tampered with or opened without your permission.

Here are a few other actions to take, before you become a target of fraud.

CREDIT FREEZE

It is easy and inexpensive to freeze your credit. Once frozen, no one can establish a new credit relationship using your identity. While this technique doesn't keep your identity private, it renders that information useless if it does fall into the wrong hands.

It takes 15 to 30 minutes to freeze. Visit each of the three credit bureaus and pay $10 for each freeze. Have available: your social security number and your addresses for the past 10 years.

- Equifax.com
- TransUnion.com
- Experian.com

Once frozen, not even you can open a credit card, get a car loan or open any credit relationship. If you need to do any of these things, you can unfreeze credit for a week at a cost of $10.

LIMIT AND SECURE CREDIT CARDS

Limit your credit cards to two major cards for 90% or more of your purchasing. One card would likely be American Express and the other either MasterCard or Visa. For each of those two cards, set up online notification so that you receive an email any time a charge is made when the card is not present.

For American Express – Go to Secure Your Account / Account Alerts / Statement and Payment Alerts / Fraud Alerts (choose email, text or both) / Irregular Account Activity / Card Not Present (online) / Cash Withdrawal

It is fine to have other cards like Nordstrom or Ann Taylor, but limit the charges to purchases for that store - online or in the store.

COPY YOUR WALLET CONTENTS

Once a year, take 15 minutes to make a copy of the contents (front and back) of your wallet. Put that copy in a safe place in your home. Then if your wallet or purse is ever lost or stolen, you will save yourself immeasurable time, anxiety and, because you can respond quickly, you rapidly shut down any fraudulent activity. If you are getting ready to travel overseas, you might leave a copy of your wallet contents with a family member or put it in the Cloud in a secure vault. Then it is accessible if you should need it. At the same time, purge your wallet of any unnecessary personal information.

If you are the victim of any type of identity theft, immediately contact Resource Consulting Group so we can help you take the appropriate steps to protect your investment accounts.