Be Vigilant about Identity Theft

Identity theft is one of the fastest growing crimes in America affecting millions of unsuspecting individuals each year. A dishonest person who has your Social Security number can use it to obtain tax and other financial and personal information about you.

Identity thieves can get your Social Security number by:

- Stealing wallets, purses, and your mail.
- Stealing personal information you provide to an unsecured website, from business or personnel records at work, and from your home.
- Rummaging through your trash, the trash of businesses, and public trash dumps for personal data.
- Posing by phone or email as someone who legitimately needs information about you, such as employers or landlords.

Tax-related identity theft occurs when a thief uses your Social Security number to file a tax return and claim a fraudulent tax refund. In 2015 alone, the IRS stopped 1.4 million confirmed identity theft tax returns, protecting $8.7 billion in taxpayer refunds.[1] The IRS has become increasingly diligent in its efforts to thwart identity theft with a program of prevention, detection, and victim assistance. The "Taxes. Security. Together." program is aimed at building awareness among taxpayers about the need to protect personal data when conducting business online and in the real world.

Stay Vigilant

By remaining vigilant and following a few commonsense guidelines, you can support the IRS in keeping your personal information safe. Here are a few tips to consider:

- Protect your information. Keep your Social Security card and any other documents that show your Social Security number in a safe place.
- DO NOT routinely carry your Social Security card or other documents that display your number.
- Monitor your email. Be on the lookout for phishing scams, particularly those that appear to come from a trusted source such as a credit card company, bank, retailer, or even the IRS. Many of these emails will direct you to a phony website that will ask you to input sensitive data, such as your account numbers, passwords, and Social Security number.
- Safeguard your computer. Make sure your computer is equipped with firewalls and up-to-date anti-virus protections. Security software should always be turned on and set to update automatically. Encrypt sensitive files such as tax records you store on your computer. Use strong passwords and change them routinely.
- Be alert to suspicious phone calls. The IRS will never call you threatening a lawsuit or demanding an immediate payment for past due taxes. The normal mode of communication from the IRS is a letter sent via the U.S. postal service.

- Be careful when banking or shopping online. Be sure to use websites that protect your financial information with encryption, particularly if you are using a public wireless network via a smartphone. Sites that are encrypted start with "https." The "s" stands for secure.
- Google yourself. See what information is available about you online. Be sure to check other search engines, such as Yahoo and Bing. This will help you identify potential theft sources and will also help you maintain your reputation.

Fear You Have Been Scammed?

If you feel you are the victim of tax-related identity theft - e.g., you cannot file your tax return because one was already filed using your Social Security number - there are several steps you should take.

- File your taxes the old-fashioned way—on paper via the U.S. postal service.
- Print an IRS Form 14039 Identity Theft Affidavit from the IRS website and include it with your tax return.
- File a consumer complaint with the Federal Trade Commission (FTC).
- Contact one of the three national credit reporting agencies -- Experian, Transunion, or Equifax and request that a fraud alert be placed on your account.

If you have been confirmed as a tax-related identity theft victim, the IRS may issue you a special PIN that you will use when e-filing your taxes. You will receive a new PIN each year.

For more information on tax-related identity theft visit the IRS website, which has a special section devoted to the topic.

Credit Freeze

Consumer advocates suggest that freezing your credit may be prudent step to also help protect your credit. The main purpose for freezing your credit is to stop identity thieves from opening accounts in your name. Once the freeze is in place, it prohibits the three consumer reporting agencies (Equifax, Transunion and Experian) from disclosing the information in your report to any new creditors. The freeze does NOT restrict existing credit accounts and existing creditors will still have access.

Legislation signed earlier in 2018 also requires that reporting agencies freeze your credit upon request without a fee. You are entitled to 3 credit freezes within a 12-month period. However, it is important to be cautious as these firms also try to sell credit monitoring or credit “locks.” Freezing your credit should not have a negative impact on your credit score.

The main reason many consumers have not taken this step proactively prior to now is that there has been a cost to freeze your credit report. Thus, given the three credit agencies you had to pay three times to freeze and three time to unfreeze, when needed. Now that the cost has been eliminated, the only real impediment is the inconvenience associated with removing the freeze when you are applying for new credit. The freeze removal can take up-to 3 days so you do need to plan ahead.

You will also set a PIN number when your account is frozen which is used to unfreeze your credit report. When opening a new account, the creditor may use one of the three services so you may only need to unfreeze one.

Now that you want to take action, what are the steps? You need to call or login to ALL three reporting agencies listed below. You will receive a PIN number so that you can unfreeze your credit.

- Equifax 1-800-685-1111 https://www.Equifax.com/personal/credit-report-services
- Transunion 1-888-909-8872 https://www.transunion.com/credit-freeze
- Experian 1-888-397-3742 https://www.experian.com/freeze/center.html

Don't forget to do for your spouse if married. You can freeze your children's credit also. Sadly, their identity may be misused as well.

Freezing you credit does not guaranty that your identity cannot be stolen. Given the limited inconvenience as well as being free, it seems to make good financial sense to take action. Now if someone can figure out how to effectively save all our passwords we will be all set!

Source/Disclaimer:

[1]The Internal Revenue Service, "How Identity Theft Can Affect Your Taxes," IRS Summertime Tax Tip 2016-16, August 8, 2016.