HOW TO KEEP INFORMATION SECURE TO AVOID IDENTITY THEFT

Nowadays, it seems everyone lives in fear of their identity being stolen – and most of us know someone who has been a victim.

The Federal Trade Commission details the four primary areas that you should oversee to ensure your personal information is secure to avoid becoming a victim yourself.

1. KEEP YOUR PERSONAL INFORMATION SECURE OFFLINE.

- Lock financial documents and records in a safe place at home, and be sure nothing is out in the open that a worker or other visitor might come across.
- At work, lock your wallet or purse in a safe place.
- Limit what you carry when you go out. Take only the identification and credit cards you need. Never take your Social Security card or anything with your Social Security number on it, such as a Medicare card. The FTC recommends that those who have Medicare cards make a copy of it and black out all but the last four numbers of the Social Security number.
- If you are asked to share your Social Security number or other personal information at a business, school or doctor's office, ask why they need it and how it will be protected.
- Shred any documents that contain personal information, including old credit cards, credit applications, receipts, insurance forms, physicians' statements, checks, bank statements, etc.
- Don't share health plan information with anyone who offers free products. Destroy labels on old pill bottles.
- Take outgoing mail to a post office collection box. Promptly remove mail from your mailbox.
- Don't have new checks mailed to your home mailbox unless it is secured.
- Consider opting out of credit card and insurance offers. Call (888) 567-8688.

2. KEEP YOUR PERSONAL INFORMATION SAFE ONLINE.

- Don't give out information online unless you have initiated the contact. If someone contacts you, rather than respond, go to the company's website and talk to a customer service representative.
- Before you dispose of an old computer, get rid of all personal information on it using a wipe program.
- When you dispose of a mobile phone, find out how to delete all information permanently. Be sure to delete everything, including phone lists, text messages, voicemails, etc.
- Use encryption software to safeguard online transactions. Look for a "lock" icon on your browser before transmitting personal information.
- Use strong passwords, particularly on bank and credit sites, and keep your passwords private.
- Don't put too much information out on social network sites. It might give away challenge questions on your financial sites. Never post your full name, phone number, address or Social Security number.

3. ALWAYS KEEP YOUR SOCIAL SECURITY NUMBER SECURE.

If someone asks for your or your child's Social Security number, ask:

- Why do they need it?
- How it will be used?
- How will they protect it?
- What happens if you don't share the number?

4. KEEP YOUR DEVICES SECURE.

- Install anti-spyware, anti-virus software and a firewall.
- Don't open phishing emails or download programs sent by strangers.
- Before using WiFi in a public place, ask to be sure the site is protected.
- Avoid putting personal information on your laptop and always lock it when you're not using it. Don't use the automatic login feature that would make it easy for a thief to login.
- Read privacy policies of organizations you do business with. Ask questions if you have doubts of their security.

Should you have questions regarding identity theft or need help filing Form 14039 (Identity Theft Affidavit) with the IRS, please give us a call at 251.473.5550 or send an email to info@rtbh.com. For other identity theft resources, we recommend visiting the following website www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft.