How to Protect Yourself From Identity Fraud

Identity theft is a growing and expensive problem in America that can happen to anyone. The Bureau of Justice Statistics estimates that about 16.6 million Americans were victims of identity theft in 2012. Combined, these victims suffered nearly $25 billion in losses, or an average of $9,650 each.[i] What isn't captured by these statistics is the time, hassle, and emotional distress of repairing the damage.

Identity theft happens when criminals steal personal information like your name, Social Security number, or financial information and use it to open fraudulent accounts or commit crimes. Though most victims are not held personally responsible for fraudulent charges, financial misdeeds done under your name can leave black marks on your credit report and linger for years after the initial theft. Follow these everyday safety tips to help mitigate the risk of identity fraud.

A Social Security number is the most commonly used piece of data to commit identity theft. Avoid giving out your Social Security number as much as possible. If you are filling out paperwork that asks for that information, find out whether you can provide an alternate form of identification instead.

Never give out personal information in response to unsolicited phone calls, emails, or letters. Do not click on links that appear in suspicious emails or enter financial information into a website linked from an email. These phone calls and emails are typically "phishing" scams attempting to draw out personal information. If you receive an account alert or other urgent message from a financial institution or government agency, call the official number listed on their website to verify the legitimacy of the request.

Shred your financial statements, old checkbooks, credit cards, and any paperwork that contains personally identifiable information like account numbers or your Social Security number. According to insurance claim data, only about 15 percent of identity theft happens online; the rest happens when thieves find personal data in your trash, home, or automobile.[ii] We host regular shredding parties at our offices so that clients and friends have a safe and secure way to dispose of sensitive paperwork. Please call our office for an invitation to the next party.

When traveling, be careful when accessing bank accounts, email, or social media accounts on public computers. It's very common for fraudsters to install key logging software that can capture passwords, login credentials, and other sensitive information. If you are forced to use a public terminal, always log out of your accounts when your session is finished and change your passwords when you return home.

Scrutinize your credit report each year for errors and accounts that have been opened in your name. You can access your record at each of the credit reporting agencies for free once per year at www.annualcreditreport.com or by calling the

Federal Trade Commission's hotline at 877-322-8228. Don't be tempted by other sites offering a free credit report; they will often sign you up for expensive credit monitoring services.

Empty your wallet and purse of extra credit cards, debit cards, old driver's licenses, Social Security cards and any other sensitive documents. Never carry passwords or account information in your wallet.

Check your bank account and credit card statements regularly to spot unusual transactions and notify your bank and credit card company when you'll be traveling so that they can be on the alert for suspicious activity.

If you believe that you may be the victim of identity theft, there are several steps you should follow to protect yourself and start the dispute process.

1. Your first stop should be to place a fraud report with the three credit reporting agencies. This will block thieves from opening any more bank or credit accounts in your name. You can contact the credit agencies at the below numbers:

- TransUnion: 1-800-680-7289
- Equifax: 1-800-525-6285.
- Experian: 1-888-EXPERIAN (397-3742).

2. Contact the relevant financial institutions to freeze or close the accounts that were compromised or opened fraudulently.

3. File a report with your local police department to document the details of the crime. Most banks and credit card companies require an official police report in order to reverse fraudulent charges.

Identity fraud can be aggravating, expensive, and time consuming, and the effects can linger for years. Following the simple safety tips we've outlined can help you or your loved ones from becoming victims of unscrupulous identity thieves. In the wake of a few high-profile data breaches financial services companies are taking identity theft very seriously and have instituted a number of safeguards to protect your information. If you'd like to know more about how your bank and brokerage accounts are protected, speak with your financial advisor.

---

[i] Victims of Identity Theft, 2012; Bureau of Justice Statistics. http://www.bjs.gov/content/pub/pdf/vit12.pdf (Accessed June 13, 2014)

[ii] Preventing Offline Identity Fraud; Travelers. https://www.travelers.com/prepare-prevent/home/identity-theft/prevention-tips.aspx (Accessed June 13, 2014)