MARCH 2018

THE FIDUCIARY GROUP
INVESTMENT MANAGERS
A FOCUS FINANCIAL PARTNER

The INDEPENDENT ADVISOR

Monthly Articles from The Fiduciary Group

Identity Theft

Brendan Flaherty
Director of Operations
brendan@tfginvest.com

Most people have been, or know someone who has been, affected by identity theft. It happens to those in their 20's, those in their 90's, and to all ages in between. According to the Federal Trade Commission, identity theft occurs when someone uses personally identifying information (PII) without permission to commit fraud or other crimes. How criminals obtain or use your data varies from incident to incident. Cyber-attacks against firms like Yahoo! and Equifax have exposed sensitive client account information ranging from social security numbers to email login credentials. The Equifax incident alone exposed PII of nearly half of the United States population.

Besides taking obvious cybersecurity steps like having anti-virus protection on each computer, there are a few things that can be done to help protect yourself. This article walks through a few steps to help mitigate the risks of having your identity stolen. These are broken down into three main groups including cyber security, physical security, and monitoring. Steps to take if identity is stolen are reviewed as well.

Cyber Security

First, watch out for phishing scams where criminals mock the emails of legitimate businesses or government agencies. Typically, the goal of these scams is to trick the person into providing sensitive information or to gain access inside the recipient's computer. This is usually done by getting the recipient to click on a hyperlink or respond with personal information. Prior to acting on an email, double check the email address it's being sent from. Even though it may say "Apple Store" next to "From," the email address could be absjfv@gmail.com. This is a red flag that the email is not legitimate.

Another critical action to take prior to clicking on a hyperlink within an email is to check the URLs within the email body. If you hover your courser over a link, the URL should display just above it or near the bottom left of the window or browser. Make sure to hover only! Do not click the link when trying to confirm the URL. This can answer the question of "where will this link take me". Typically, legitimate website URL's will include HTTPS as opposed to HTTP. In the below example, hovering over the "CLICK HERE" link exposes the website as http://abc123.com as opposed to a SunTrust based website.

Hi,

Please click the link below to gain access to your account.

http://abc123.com/
Ctrl+Click to follow link

CLICK HERE

Thank you,
SunTrust

In the second example below, next to "From" appears to be "OFFICE". The sender is posing as Microsoft Office, but the actual email is not Microsoft related, as seen below. This can be viewed by clicking on "From" to reveal the true email address. This is a red flag that the sender is not who they are posing to be and might be phishing for personal data.

From: OFFICE <mlceball@sat.gob.gt>
Sent: Tuesday, February 13, 2018 8:33:44 AM
Subject: Regain your inbox access

Do not log into sensitive online accounts from a public or unfamiliar computer. According to Microsoft, public computers are at risk of tracking software that is able to track each click, screen, and history. This includes the usernames and passwords of accounts that have been logged into using that computer.

When making online purchases, it is best to use a credit card as opposed to a debit card. Credit card companies must follow stringent consumer protection laws which can benefit the consumer in a fraudulent charge situation. According to AARP, because the money hasn't left the account like using a debit card, consumers will have more leverage with the credit card company with fraudulent activity.

Physical Security

There are additional actions you can take that are more physical in nature and less to do with cyber security or technology. For instance, ATM receipts, credit cards, statements or anything with sensitive information should not be thrown out in a usable form. They should always be torn up and ideally shredded.

Some individuals also carry their Social Security Card in their wallet or purse. This is not recommended as the card is at risk of being stolen. Never give your credit card information over the phone unless you are the one who initiated the call. Scammers might obtain a key piece of information to gain your trust, then call you to obtain sensitive information like a credit card number. Posts or profiles from social media sites can be used against you like address, phone numbers, or even vacations. Keep this in mind when engaging in social media.

Monitoring

Even when following the previously mentioned steps to reduce the possibility of identity theft, there is always a chance it still occurs. Reviewing and reconciling your bank account balances and transactions weekly is a good way of monitoring activity. Log in and check your credit card activity every few days, and at least weekly. If fraudulent activity occurs, you should be able to spot it within days. Another proactive way to monitor is to read your credit report. The main reporting agencies (Equifax, Experian and TransUnion) are legally obligated to provide you with a report annually, so you should be able to request one every four months from one of the three. Review the report to ensure its accuracy including credit related detail, but also personal data like name, address etc. Some individuals take the extra step to sign up for a credit monitoring service. This service typically will scan activity as it relates to your credit and notify you when an application is submitted, such as a credit card application.

Post Identity Theft Event

According to Equifax, there are six steps to complete in the unfortunate event of identity theft.

1. Contact the company or institution(s) where the identity theft occurred. If a fraudulent charge occurred on your credit card, contact the credit card company. Speak with their fraud department to take immediate steps and to leverage their expertise.

2. Create a fraud alert at the credit reporting agencies. You can either notify them individually, or contact Equifax who should be able to notify the other two.

3. Lock your credit reports at the three main credit reporting agencies (Equifax, Experian and TransUnion). This will help to stop accounts from being opened in your name because the firm is usually required to pull your credit. You can place a temporary lift on the credit freeze in the situation where you need to open new lines of credit or new accounts.

4. File an affidavit with the TFC, which can be done through https://www.identitytheft.gov. The FTC can help provide additional steps when an identity is stolen.

5. File a police report with your local department and obtain a copy of this report. You should also disclose your FTC serial number obtained in the step above. According to the FTC, this will help obtain the legal benefits of someone who has gone through identity theft.

6. Monitor your accounts and credit reports for any fraudulent activities. This is an ongoing precaution to catch any further issues sooner rather than later.

The first lines of defense against identity theft are the actions you take. Staying vigilant with your online and physical data can help reduce the chances of something happening. Simply having this in mind can go a long way.