FEBRUARY 2019- PROTECTING AGAINST FRAUD AND IDENTITY THEFT

The *Financial Principles Guidebook* is a comprehensive collection of our planners' insights to help you along your pursuit of financial independence.

IN THIS GUIDEBOOK

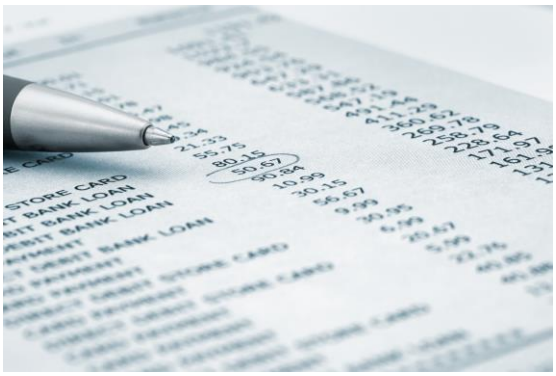
According to Javelin Strategy and Research's 2018 Identity Fraud study, there were over 16.7 million victims of identity theft in 2017, with over $16.8 billion stolen from victims. As technology continues to advance, unfortunately so does the amount (and sophistication) of cybercrimes.

We have prepared this *Guidebook* to provide actionable tips to protect yourself from fraud and identity theft, along with the steps to take if you are a victim.

***We hope that you find this information valuable. Should you have any questions, please do not hesitate to contact our office. If you have a friend, family member, colleague, or client who may benefit from this Guidebook, please do not hesitate to share it with them*.**

FOCUSED ON YOUR FINANCIAL INDEPENDENCE

HAVE YOU BEEN THE VICTIM OF IDENTITY THEFT OR FRAUD?



In 2017, 145 million Americans had their personal information accessed in the largest data security breach ever at Equifax. Millions more had their personal information exposed in recent years by breaches at JP Morgan Chase, Target, and Uber. These breaches are becoming more frequent and, as technology continues to advance and become more sophisticated, unfortunately, so do the cybercriminals who try to use your personal information for profit.

One of the easiest and best ways to identify identity theft and fraud is to simply monitor your statements, mail, and credit reports. Unfortunately, surveys show that nine out of ten people don't regularly check their financial statements. The longer you do not know that you have been the victim of a cybercrime or identity theft, the greater the damage can become. You should regularly review your account statements and credit report to identify irregularities.

WARNING SIGNS THAT YOU MAY BE THE VICTIM OF IDENTITY THEFT

- Charges for goods or services that you did not purchase appear on your credit card or bank statements.
- A statement for an unknown credit card or other loan turns up in your mail.
- A credit card that you did not apply for comes in the mail.
- You receive a collection notice or phone call for a debt that you do not recognize.
- There are errors, or accounts you do not recognize, on your credit report.
- You have good credit but an application for credit is denied.
- You stop receiving a statement for a credit card or bank statement (a thief may change the address on an account in an attempt to keep you from noticing their crime for as long as possible).
- The IRS notifies you that more than one tax return was filed in your name or that you have income from a company that you do not work for.
- Your wallet, cell phone, credit card, debit card, or computer were lost or stolen.

ARE YOU REVIEWING YOUR ACCOUNT STATEMENTS?

With the rise of electronic transfers and autopayment of bills, it is becoming easier and faster to complete financial transactions. Unfortunately, the easier it is to link credit cards and other debts to bank accounts, the less closely consumers are monitoring their statements. Often, identity theft will start with a few small charges or withdrawals to "test" an account. You should set aside fifteen minutes once a month to review your bank and credit card statements to identify unauthorized charges. Additionally, most online credit card and bank accounts offer customizable account alerts, which only take a few minutes to set up, and will allow you to receive alerts when unusual (or even regular) activity occurs on your account. It's a great tool to catch fraudulent or erroneous charges.

WHEN WAS THE LAST TIME YOU REVIEWED YOUR CREDIT REPORT?

If a thief has opened a credit card account or other debt in your name, it will likely appear on your credit report. You should check your credit report at least once per year to make sure that the information is correct and that your credit history is accurate and up to date. You are entitled to a free copy of your credit report from each of the credit bureaus (Experian, Equifax, and Transunion) once per year. We recommend that you review one report every four months. For example, you can review Experian this month, Equifax in June, Transunion in October, and start all over again next year. You can access your credit report at www.annualcreditreport.com or by calling 877-322-8228.

What to do if you have been the victim of identity theft

Whether someone has made an unauthorized charge using your credit card or taken out a loan using your credit, it is important that you act quickly to stop the thief's activity and then reverse any potential damage.

Lockdown the problem account

An unauthorized transaction in a financial account is often the first red flag that you have been the victim of identity theft. If there is an unauthorized transaction in one of your financial accounts, contact the financial institution, dispute the transaction, and lock or close the account.

Review your credit card statements, bank statements, and credit reports

Review all of your open financial accounts to identify any other potential unauthorized activity. Then review your credit reports to confirm that the thief hasn't opened any new credit accounts in your name. If there are any opened debts that you are not aware of, contact the creditors immediately.

File a report with the Federal Trade Commission and your local police department

You should start to create a paper trail to document the theft. If you visit www.identitytheft.gov you will be able to file a report with the Federal Trade Commission (FTC). This report will also come with a recovery plan and prefilled letters and forms that you can use to file police reports and dispute fraudulent charges. In addition to filing a report with the FTC, you should contact your local police department.

Place a fraud alert on your credit reports

Contact all three credit bureaus and ask that they place a fraud alert on your credit report. When you contact one credit reporting bureau, they should notify the other two. However, we recommend that you contact all three. This alert will initially last 90 days, and it will notify all institutions that pull your credit report that your identity has been compromised.

Open new credit accounts and financial accounts

You should speak with your financial institutions to determine how best to avoid future damage. In most cases, that will involve closing and reopening accounts. This can be a tedious process, but it is important to avoid a thief from doing further damage.

Consider a Credit Monitoring Service or a Credit Freeze

If your information was accessed in a data breach, you may want to sign up for a free subscription to a credit monitoring service. For example, Credit Karma is a reliable and free credit monitoring service, and some credit card companies, such as Capital One, Chase, and Discover, offer credit monitoring services as part of their accountholder benefits. These services monitor your credit reports for suspicious activity and sends alerts whenever a new account is opened.

You can also freeze your credit. A credit freeze will cut off access to your credit report meaning that no new accounts are able to be opened. If you are opening a new credit card account or making a large purchase such as a home or car, you would need to unfreeze your credit to allow the transaction. You can freeze your credit by calling each of the three reporting agencies: Equifax: 800-685-1111, Experian: 888-397-3742, Transunion: 888-909-8872.

Tips for Avoiding a compromise and Safeguarding your Identity

Do you have strong passwords?

Having a strong password goes a long way to keeping hackers out of your email and financial accounts. You should make passwords difficult and should never include your name, your pet's name, your children's name, or a birthday in your password. Passwords should also be updated at least twice per year. A great trick to creating a secure password that is easy to replace letters with symbols. For example, strongpassword could be replaced with $tr0ngp@$$w0rd where S is replaced with $, O is replaced with a zero, and A with @. **You should always ensure that your smart phone and computer are locked with a passcode.**

Be careful opening emails from unknown senders and always use secure email

Be very careful opening emails and attachments from unknown senders. You should also never share personal information such as a social security number, credit card number, or bank information over email. If you are exchanging personal information over the internet (such as with your accountant or financial advisor) be sure that a secure file sharing service is being used.

Don't access secure websites from a public computer

You should be careful not to access secure websites such as your bank, credit card, or social security from a public computer (library, coffee shop, etc.).

Install anti-virus software, and keep it up to date

Don't keep a password list for all of your accounts

With more and more of our lives being pushed online, we have more and more logins for various websites. They can be hard to manage. While it is tempting to keep a password list, resist the temptation. If your password list is compromised, so are all your financial accounts! If you are having a hard time managing all your logins, there are secure password management software that you can use (such as dashlane, StickyPassword, and RememBear).

Be careful of phone scammers

There are a lot of scams that are being conducted over the phone. Below is a list of some of the common ones.

"This is the IRS calling…" one of the most common phone scams involves someone calling you impersonating the IRS. They can say that you owe them money, or that they want to send you money that they owe you. They will generally ask for your banking information to make a transaction. Don't fall for it!

Medicare or health insurance- a phone scam that targets mostly seniors and involves enrollment in health insurance or obtaining a new insurance card in exchange for your social security number.

"This is Microsoft calling…." another common phone scam includes customer service support people, generally technology assistance, for a compromise to your computer. These scammers will generally ask you to allow them remote access to fix your computer. Don't do it! The thieves when they access a computer will try to steal personal and financial information.

Use common sense

If something ever just doesn't seem right, proceed with caution! Remember, creditors and government agencies won't call and ask you for your personal information, they will only confirm your personal information when you call them.

Have a topic you want to see covered in The Guidebook?

Call or email your advisor with a suggestion for a topic to be covered in The Guidebook. If we have covered it, we will send you that edition. If we haven't covered it, we will!

Have a friend, neighbor, coworker, or relative who could benefit from this Guidebook?

Feel free to forward our Guidebook to anyone you feel would benefit from this information. We would be happy to speak with them and answer any questions that they may have.

HIGHTOWER
FINANCIAL PRINCIPLES, LLC

Financial Principles, LLC
A HighTower Wealth Management Practice

310 Passaic Avenue, Suite 203, Fairfield, NJ 07004
505 Fifth Avenue, 4th Floor, New York, NY 10017
973-582-1000
www.financialprinciples.com

Focused on your Financial Independence

Bradley H. Bofford, CLU®, ChFC®, CFP®
Managing Director, Partner
973-582-1002
bbofford@hightoweradvisors.com

Michael Flower, CFP®
Managing Director, Partner
973-582-1004
mflower@hightoweradvisors.com

Daniel Trout
Partner
973-582-1006
dtrout@hightoweradvisors.com

Steven Gelber, AIF®
Associate Wealth Advisor
973-582-1015
sgelber@hightoweradvisors.com

Andrew Olivier, CFP®
Associate Wealth Advisor
973-582-1005
aolivier@hightoweradvisors.com