



Taylor Financial Group's Monthly Planning Letter



Identity Protection Month

Have you ever received an email from a “friend” or “member of a foreign royal family” who is stranded in a foreign country? They lost their wallet and passport and their only form of communication is email. They are reaching out to you in desperate need of a wire transfer for a plane ticket home.

Have you ever received a call from the “IRS” where a fake IRS agent demands money from you or states that you will be arrested? It is important to note that the IRS does not ever call to demand immediate payment using a specific payment method such as a prepaid debit card, gift card, or wire transfer!

These are common scams run by scammers. **Cyber crimes are on the rise and unfortunately another American falls victim of identity theft every two seconds** (Source: Insurance Information Institute, 2015). According to a 2018 online survey by the Harris Poll, nearly 60 million Americans have been affected by identity theft.

As email phishing attempts and hackers become more sophisticated, consumers must be more vigilant than ever before.

We have prepared this short newsletter to help protect your credit scores, increase your cyber security, and hopefully help to protect you from identity theft and other cyber crimes.

In this Issue...	Page
Why you need to review your credit report annually	2
How to create stronger passwords	
How to keep track of your many passwords	
Credit monitoring versus credit freezes	3
How to know if your identity has been stolen	
What to do if you are the victim of identity theft	4
The identity theft prevention checklist	5

Securities offered through Cetera Advisor Networks, Member FINRA/SIPC.
Investment Advice offered through CWM, LLC, a registered investment advisor.
Cetera Advisor Networks is under separate ownership from any other named entity.

The opinions voiced in this material are for general information only and are not intended to provide specific advice or recommendations for any individual.
Information Disclosure: The information contained herein has been obtained from sources considered to be reliable, but accuracy or completeness of any statement is not guaranteed.

© Taylor Financial Group. All Rights Reserved.

When was the last time you reviewed your credit report?

You may have been the victim of identity theft, and not even know! Somebody may have used your name and credit history to finance a large purchase (which mind you they may have no intention of paying for). **You should review your credit report at least annually to identify not only mistakes that may affect your credit, but fraudulent purchases or transactions.** Your credit report will include account information (like credit cards and installment loans), personal identification information (like names, addresses, date of birth, and phone numbers), and a list of any requests for your credit history.

You are entitled to one free copy of your credit report from each of the three credit bureaus every 12 months. You can retrieve a free copy of your credit report from each of the three large U.S. credit bureaus (Equifax, Experian and TransUnion) at AnnualCreditReport.com.

You can also request that a copy of your credit report from each of the three bureaus be mailed to you by calling 1 (877) 322-8228. You should check your credit reports at least once per year so that you can identify and resolve any inaccuracies in a timely manner.

Do you have strong passwords?

“I’m sorry, your password does not meet our minimum-security standards of eight characters, an upper-case letter, a lower-case letter, a number, and a special character.” How many times have you been annoyed by this message?

Having strong passwords is the first line of defense to keeping hackers out of your email accounts, and even worse your financial accounts. Passwords should never include your name, birthdate, pets’ names, or other easily identified personal information. **Your passwords should always be unique and should be updated every 3-6 months.** A clever way to strengthen your password is to use a mnemonic device or to convert letters or words to symbols (such as “S” to “\$,” “to” to “2,” or “at” to “@”). For example, when using a mnemonic device to create a password, the statement “I will spend Sundays at the beach to relax” can be easily remembered and converted to a secure, unique password by using the first letter of each word and converting applicable words to symbols. The resulting password, which would be difficult to hack, would be “IwsS@tb2r.”

Having trouble managing all of those strong passwords?

Do you ever feel like you have a hundred logins to different websites and accounts? Ever feel like they all have different password requirements and you just can’t remember all of those logins and passwords? You may be tempted to write all of those passwords down on a piece of paper or create an Excel spreadsheet with all of your logins. This is not a secure way to manage all of your passwords and logins. In fact, doing so increases your risk of a security compromise!

There is software available that can help you manage all of your passwords and logins securely. [Please click here](#) for Consumer Advocate’s review of the Top 10 technologies for password management. We at TFG are fans of True Key. True Key is software that you can install on your computer and phone to automatically store your logins for websites. You can also access the software remotely. It is free to save the first 15 passwords and costs only \$19.99 per year for an unlimited number of logins (well, up to 10,000).

Links to third party websites are not endorsements and we make no representations as to the completeness or accuracy of information provided by third parties. The opinions voiced in this material are for general information only and are not intended to provide specific advice or recommendations for any individual.
Information Disclosure: The information contained herein has been obtained from sources considered to be reliable, but accuracy or completeness of any statement is not guaranteed.

What is the difference between a credit freeze and credit monitoring?

A credit freeze will put a “lock” on your credit. This means that no new accounts can be established with any lenders using your identity. If you should want to open a new account in the future, you will need to contact the credit reporting agencies, unfreeze your credit, open the new account, and then contact the credit reporting agencies again to freeze your credit. This is the most secure way to ensure that nobody opens a new account using your identity. There are nominal fees associated with freezing and unfreezing your credit.

Credit monitoring services will alert you when new accounts are established in your name, or when there is unusual activity on your credit report. These services are subscription services (generally between \$10 and \$30 per month).

For most clients, freezing your credit is a cheaper and more secure option. However, if you have several credit cards and accounts or plan to open new accounts in the short term (a mortgage refinance, a car lease, a new credit card, etc.), continually unfreezing and refreezing your credit reports could become a costly hassle. Therefore, a credit monitoring service may be a better option for you. [You can click here to read Consumer Advocate’s reviews of their Top 10 ranked credit monitoring services.](#)



What are the signs that I may have had my identity stolen?

- **Calls or letters from creditors or collection agencies demanding payment for items that you never bought or for accounts that you never opened.**
- You aren't receiving mail for all of your financial accounts.
- You read information in your credit file about accounts that you never opened.
- Calls from creditors, or potential creditors, about suspicious new accounts, a large volume of credit card activity, wire transfers, etc.
- Unauthorized withdrawals from and transactions in bank accounts.
- **Your wallet, purse, or cell phone is lost or stolen. Ditto for paycheck stubs and credit card receipts.**
- Credit card or telephone bills do not arrive on time as regularly scheduled (your mail may have been diverted to another address).
- **You received a credit card or statement for an account that you did not open.**
- Replacement credit cards have not been received prior to the expiration date on previous cards.

What should I do if I am the victim of identity theft?

Step 1: Stop the imposter's activity!

- **Obtain a copy of your credit report from all three credit reporting agencies.**
- **Review the credit report and identify all financial accounts.**
 - Contact all financial institutions and have new account numbers issued.
 - Highlight all accounts that you did not open and send a copy of the highlighted report to each credit reporting agency with a letter explaining that you did not open the highlighted accounts:
 - Equifax- P.O. Box 105069, Atlanta, GA 30348
 - Experian- P.O. Box 9554, Allen, TX 75013
 - TransUnion- P.O. Box 6790, Fullerton, CA 92834

Step 2: Report the Crime to the Federal Trade Commission and Local Law Enforcement

- **Make an online report to the Federal Trade Commission www.ftc.gov/idtheft.** On the FTC website, you will find an "ID Theft Affidavit." You should print it, sign it, and keep a copy for your future use. If you are filing an online report, you should request that an "ID Theft Affidavit" be mailed to you.
- **Contact your local police, sheriff or other law enforcement where you live to file a report.** You should provide the police with a copy of the highlighted fraudulent activity on the credit report, or on any credit card or bank statements, false signatures on receipts or application forms, collection letters, and the FTC ID Theft Affidavit to be attached to the police report. Get a copy of the police report for your records.

Step 3: Repair the Damage

- Keep a log of all phone calls and attempts to clear up identity theft. Include date, time, and the person you spoke with by phone and then follow up in writing.
- **File disputes of fraudulent activity with credit reporting bureaus and ask that disputed items be blocked or removed from your credit report.** Notify the FTC if credit bureaus fail to block disputed items from your credit report.
- Contact companies where fraud or imposter accounts were opened.
- Send a written dispute to the fraud department along with a copy of the ID Theft Affidavit, police report, and proof of your identity
- **Close or freeze these accounts.** Request a confirmation letter that these accounts are closed or frozen
- Request copies of account information, applications, and other related business records:
 - Companies must comply with a request for information within 30 days at no cost or a subpoena. A copy can also be sent to the law enforcement agency handling the investigation upon your request. (The Right to Obtain Documents FCRA section 609(e)).
 - An imposter can use personal information to obtain credit, employment, social security, medical services, IRS refunds, or even avoid criminal arrest or action. If someone has assumed your identity or committed imposter fraud, then visit www.idvictim.org for a tool kit.

The opinions voiced in this material are for general information only and are not intended to provide specific advice or recommendations for any individual.

Information Disclosure: The information contained herein has been obtained from sources considered to be reliable, but accuracy or completeness of any statement is not guaranteed.

© Taylor Financial Group. All Rights Reserved.

The Identity Theft Prevention Checklist

- Don't access secure websites, such as online banking, from shared computers or in public.
- Ensure that your passwords are strong and that they are reset every 3-6 months.
- Ensure that your social networking profiles only share information with those who you trust.
- Only provide your Social Security number when absolutely necessary, such as to employers, tax professionals, or banks.
- Be careful opening emails (and attachments) from unknown email addresses or senders, or from friend's accounts, which may have been hacked.
- Check the security of online stores before you purchase goods.
- Shred all sensitive information before throwing it in the garbage.
- When sharing personal information, such as with tax preparers or mortgage lenders, be sure to do so through secure email or document delivery.
- Enroll in fraud alerts. Most banks and financial institutions offer fraud alerts where you can receive emails, phone calls, or text messages when there is suspicious activity related to your accounts.
- Install anti-virus software on your computer and ensure that it automatically checks for software updates.
- Ensure that your phone, computers, tablets, and other devices are password protected.

At Taylor Financial Group, we take the security of your financial and personal information very seriously. To that end, we will never:

- Share your personal information with third parties without written approval
- Email copies of your statements, tax documents, or other personal information, to you or any authorized third party without utilizing email encryption
- Release funds from your accounts without verbally confirming withdrawal instructions with you first
- Execute on trading instructions that have not been verbally confirmed.

Should you have any questions, please do not hesitate to contact our office!

Taylor Financial Group, LLC

795 Franklin Avenue

Suite 202, Building C

Franklin Lakes, NJ 07417

(201) 891 – 1130

office@taylorfinancialgroup.com



Securities offered through Cetera Advisor Networks, member FINRA/SIPC. Investment advice offered through CWM, LLC, a registered investment advisor. Cetera Advisor Networks is under separate ownership from any other named entity.

The opinions voiced in this material are for general information only and are not intended to provide specific advice or recommendations for any individual.
Information Disclosure: The information contained herein has been obtained from sources considered to be reliable, but accuracy or completeness of any statement is not guaranteed.

© Taylor Financial Group. All Rights Reserved.