Fraud Prevention Tools

"Identity fraud is a serious issue, as fraudsters have stolen $112 billion in the past six years. That equals $35,600 stolen per minute, or enough to pay for four years of college in just four minutes." [1]

Comprehensive Wealth Management works hard to protect the privacy and security of clients. Below you will find tools for helping prevent fraud in your life.

What CWM does to protect you:

- CWM will not sell your personal information to anyone, for any reason. Please refer to our Privacy Policy, by selecting the "Privacy Policy" link on the bottom of our website at www.CWMnw.com.
- CWM uses firewall and encryption to protect your personal information on our computer systems.
- CWM employees are held to strict standards in keeping client information safe, and are regularly trained to protect client privacy and security.
- CWM will never ask you to give out your confidential information via email.

What you need to do to protect yourself:

- Be sure to provide CWM with current information to contact you if we suspect unauthorized access to your accounts.
- Continuously update your computer with the latest version of your computer's operating system, browser and security software.
- Activate your computer's firewall.
- Install anti-virus **and** anti-Spyware software
- Avoid using public computers and unsecured public Wi-Fi.
- Always log out of websites after use.
- Switch to paperless delivery where possible.
- **Never** send your personal information via email, unless you are using encryption or a secure portal (Example: A trusted CWM employee sends you a blank new account application, you print it out, complete it with all personal information, scan and email it back. In that instant, your information may have been compromised.) Be sure to closely follow instructions provided to you by those trusted individuals sending forms, applications, and requesting information.
- Never give your personal information over the phone unless you are the one that initiated the call **or** you have verified the identity of the caller. Remember: a reputable company will not contact you via email or phone to request sensitive information.
- Create unique passwords – **Do not** use sensitive or easily accessible information such as your Social Security number, date of birth, and your child's or pet's name.
- When possible, sign in using multiple verification steps such as a pin, security questions, picture ID etc.
- Change passwords regularly and use secure password managers such as roboform, lastpass, or 1password to store your passwords.
- Shred documents that have confidential financial or identification information.
- Always go directly to the website, never click on a link embedded in an e-mail.

Fraud Prevention Tools

- Conduct your own due diligence when purchasing products on-line from sites such as Craig's List – Always meet the person in a safe or public place (such as a police station) and pay with a cashier's check.
- Be cautious about what you share via Social Media - Fraudsters can piece together the information you share on social media to gain access to your accounts and property (e.g. birthdays, vacation times, children's names, locations, etc.).
- ***If you have a Schwab account*** - Schwab has an ID Theft team that can help with computer viruses, available to clients free of charge.
- Be vigilant – if you think something is suspicious it probably is.

How to prevent Firefox web browser from storing passwords:

1. In the upper right hand corner click on the three horizontal lines
2. Click "Options"
3. On the left hand side click "Security"
4. Under "Logins" uncheck the "remember logins for sites" and if you want to delete any passwords, click "saved logins" then proceed to delete saved passwords

How to prevent Chrome web browser from saving passwords:

5. Click on the 3 horizontal lines in the top right hand corner
6. Click on "Settings"
7. At the bottom click "Show Advanced Settings"
8. Scroll down and under "Passwords and Forms" uncheck the "offer to save your web passwords" box.

If you suspect identity theft or unauthorized access to your account, it is important to act quickly:

- Contact CWM at 425-778-6160 or toll free 800-268-2440
- Contact Schwab at 800-435-4000 or 602-355-7300 if you are out of the country
- Contact your bank and credit card providers

Let the credit bureaus know:

- Equifax: Call 800-525-6285 or visit www.equifax.com
- Experian: Call 888-397-3742, or visit www.experian.com
- TransUnion: Call 800-680-7289, or visit www.transunion.com

Notify the appropriate government agency:

- Visit FTC's Identity Theft site for more information, www.ftc.gov/bcp/edu/microsites/idtheft/
- Forward suspicious emails to nophising@cbbb.bbb.org

[1] Pascual, A., Marchini, K., & Miller, S. (2016, February 02). 2016 Identity Fraud: Fraud Hits and Inflection Point. https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point