McCARTHY GRITTINGER
FINANCIAL GROUP LLC

Equifax cybersecurity incident

Dear Valued Clients & Friends:

On September 7, 2017, Equifax, one of the nation's three major credit reporting agencies, announced what it describes as a "cybersecurity incident" involving consumer information affecting up to 143 million customers. According to an Equifax statement, the incident of unauthorized access occurred from mid-May through July 2017. Hackers had access to names, Social Security numbers, birth dates, addresses, driver's license numbers and credit card numbers. It is important to note that this is an Equifax incident and is not related in any way to our clients' custodians, TD Ameritrade, Charles Schwab, and Vanguard data or systems.

Following are steps to take as recommended by the Federal Trade Commission (FTC) to help protect your information from being misused. Visit Equifax's website, www.equifaxsecurity2017.com.

- Find out if your information was exposed. Click on the "Potential Impact" tab and enter your last name and last six digits of your Social Security number. Your Social Security number is sensitive information, so make sure you're on a secure computer and an encrypted network connection any time you enter it. The site will tell you if you've been affected by this breach.
- Whether or not your information was exposed, U.S. consumers can get a year of free credit monitoring and other services. You have until November 21, 2017 to enroll.

Here are some other steps to take to help protect yourself after a data breach as well as links and articles to get you started:

- **Check your credit reports** from Equifax, Experian, and TransUnion - for free - by visiting annualcreditreport.com. Accounts or activity that you don't recognize could indicate identity theft. Visit IdentityTheft.gov to find out what to do.
- **Consider placing a** credit freeze **on your files.** A credit freeze makes it harder for someone to open a new account in your name. Keep in mind that a credit freeze won't prevent a thief from making charges to your existing accounts.
- **Monitor your existing credit card and bank accounts closely** for charges you don't recognize.
- If you decide against a credit freeze, **consider placing a** fraud alert **on your files.** A fraud alert warns creditors that you may be an identity theft victim and that they should verify that anyone seeking credit in your name really is you.
- **File your taxes early** - as soon as you have the tax information you need, before a scammer can. Tax identity theft happens when someone uses your Social Security number to get a tax refund or a job. Respond right away to letters from the IRS.

Visit Identitytheft.gov/databreach to learn more about protecting yourself after a data breach.

As always-please call us with any questions or to discuss the ideas listed above about protecting yourself from financial fraud.

Your Anxiety Removal Team®

Scott D. Grittinger, CFP®
Matthew T. Miler, CPA, CFP®
Jacqueline A. Schneider, CFP®
Amy L. Finley®
Alicia A. Nordwig, AAMS®
Robert P. Kult, CPA
Maggie Mayer