

September 15, 2017

Last week, one of the big four credit reporting agencies, Equifax, announced it experienced a security breach resulting in criminals accessing personal information of approximately 143 million Americans between May and July of this year. The compromised information included names, addresses, Social Security numbers, and dates of birth. In some instances, driver's license numbers, credit card and credit dispute information were also compromised. This information is nearly everything that is needed to open an account in your name.

While my office does not have a direct relationship with Equifax, due to the sheer size of the breach, I felt it important to reach out and let you know what you can do to protect yourself.

- First, visit the Equifax breach website at www.equifaxsecurity2017.com to determine whether you have been impacted. Keep in mind that the full impact of this breach may not be known yet, so consider revisiting the site periodically for the next few weeks.
- If you are impacted, consider placing a freeze on your credit with all of the following credit reporting agencies. Freezing your credit is the only way to prevent those with your personal information from opening accounts in your name.
 - Equifax: https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp
 - Transunion: <https://freeze.transunion.com/sf/securityFreeze/landingPage.jsp>
 - Innovis: <https://www.innovis.com/securityFreeze/index>
 - Experian: <https://www.experian.com/freeze/center.html>
- Consider obtaining credit monitoring services. Equifax is offering free credit monitoring to all Americans, whether impacted by the breach or not. Several companies also offer similar services for a fee. Please note that credit monitoring does *not* prevent ID theft; it simply alerts you when events occur that may impact your credit.
- If you believe your information has been compromised, contact our office at to discuss options to further protect your investment accounts. If you wish, we can place restrictions on your account(s) that will prevent anyone from being able to effect transactions or withdrawals without our office's awareness and approval.
- Be on high alert for impersonators or phishing attempts by fraudsters. Be on the lookout for emails that appear to be from these companies, telling you that you've been impacted, or otherwise creating a sense of urgency, and to "click here" for more information. When in doubt, do not click the link. Any legitimate company will have another way for you to contact them to be sure the email is safe.

As always, thank you for your business and trust. If you have any additional concerns, don't hesitate to reach out directly.

Sincerely,

Dan L. Wilburn, CFP®
R.B. Smith Company
President

LPL Financial is not affiliated with any of the credit reporting agencies listed.

