Ginsburg Financial Advisors, Inc.
Personal Financial Planning & Investment Management
Larry P. Ginsburg, CFP® Adele Ostomel, CFP®

phone: **(510) 339-3933**
fax: (510) 339-1611
LGinsburg@GinsburgAdvisors.com
AOstomel@GinsburgAdvisors.com

The Equifax Data Breach

Have you been affected? If so, how can you try to protect yourself?

For those of you who know, and those who have yet to learn, we felt it was important to communicate with you about a recent breach experienced by Equifax, one of three major credit reporting agencies, where hackers stole the private information of millions of people that is now available for distribution to disreputable individuals anywhere in the world.

On September 7, credit reporting agency Equifax dropped a consumer bombshell. It revealed that cybercriminals had gained access to the personal information of as many as 143 million Americans between May and July – about 44% of the U.S. population. The culprits were able to retrieve roughly 209,000 credit card numbers, in addition to many Social Security and driver's license numbers.[1]

How can you find out if you were affected? Visit equifaxsecurity2017.com, the website Equifax just created for consumers. There, you can enter your last name and the last six digits of your Social Security number to find out. (Having to enter the last six digits of your SSN hints at how significant this breach is.)[2]

Given that their system has already been compromised and not knowing if you are one of the many victims, we caution you about providing part of your social security number in order to find out if you are among the victims. Equifax will be sending a letter directly to those impacted by the breach that you will receive without having to reveal more information.

If you are among the consumers whose data was hacked, Equifax will ask you to return to equifaxsecurity2017.com to enroll in an identity theft protection product, TrustedID Premier. This program will provide you with free credit monitoring for a year. (The lingering question is whether your data could be used easily by criminals afterward).[1,2]

However, this action may not be in your best interest. The fine print of the agreement to enroll may include language that could prevent you from participating in any class-action suit or arbitration that may result from this incident. At this point, it is unclear if this "opt out" clause applies to this cybersecurity incident.[3]

How should you respond? Beyond simply taking Equifax up on its offer of one year of identity theft insurance and free credit monitoring, you can take other steps.

Check your credit reports now. (Unless you have already done so in the past month). You can get one free credit report per year from Equifax, TransUnion, and Experian. To request yours, go to annualcreditreport.com.

Scrutinize your credit card and bank account statements for unfamiliar activity, and sign up for email or text alerts offered by your bank or credit card issuer(s), so that notice of anything suspicious can quickly reach you.

Consider changing the password for your main email account. A weak password on that account is a low bar for a cybercrook to hurdle – and once hurdled, that crook could potentially pose as you to change the passwords on your financial accounts.[4]

Regarding bank, investment, and credit card account passwords, avoid the obvious. Too many people use simple passwords based on their pet's name, their last name and year of birth, the high school they attended, etc. Sadly, these same simple facts are often answers to security questions for credit card and bank accounts. Ask your bank or credit card issuer if you can use additional, random words or a PIN for passwords or security question answers. That way, you can avoid logging in using data that is in the public record. For example, instead of using your mother's actual maiden name, pick your favorite vegetable as the answer to this question. You want your password to be long and random, to make it harder for a would-be thief to guess. Also, consider using hyphens and spaces along with numbers, letters, and symbols when creating a password (e.g. "–Saturn05!" or "Saturn !05").

Consider paying for additional identity theft protection for years to come. This is one way to try and shield yourself from the unauthorized use of your Social Security number, driver's license number, email accounts, and credit card numbers.

If someone calls you out of the blue claiming to be from Equifax, do not cooperate with them. Unless Equifax is returning your call, they will not contact you by phone. The same applies if you get a random, unsolicited email or text from "Equifax" – do not comply, or you may inadvertently hand over personal information to a fraudster. Stay vigilant, today and in the future.

Citations.
1 - wired.com/story/how-to-protect-yourself-from-that-massive-equifax-breach/ [9/7/17]
2 - washingtonpost.com/news/the-switch/wp/2017/09/08/after-data-breach-equifax-asks-consumers-for-social-security-numbers-to-see-if-theyve-been-affected [9/8/17]
3. www.nytimes.com/2017/09/10/smarter-living/equifax-hack-what-should-i-do
4 - cleveland.com/business/index.ssf/2017/09/devastating_data_breach_at_equ.html [9/8/17]