1919 INVESTMENT COUNSEL
Complexity to Clarity

Response to Equifax Breach

September 2017

As has been reported by multiple media outlets, last week, one of the world's largest consumer credit reporting agencies, Equifax, disclosed a massive data breach involving the personal data of 143 million people. This data breach includes the theft of the names, addresses, birth dates, social security numbers and drivers' license numbers of these individuals. It has been reported that hackers downloaded this personal information through a web application created by Equifax which was not properly secured.

1919 Investment Counsel recommends clients take the following steps to protect themselves against this data breach and others.

1. Request credit reports from all three consumer credit reporting agencies through www.annualcreditreport.com. Experian and TransUnion along with Equifax are considered the three major consumer credit reporting agencies. 1919ic recommends clients make this part of their annual review of their finances as data breaches are happening with more regularity.

2. Clients should also consider going to the Federal Trade Commission's Consumer Information web site, see link below, and review the advantages to putting a credit freeze in place at all three consumer credit reporting agencies.

   https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs

3. Beware of any email and or phone solicitations from people claiming to be part of a credit monitoring agency or from a similar type of company offering assistance with credit checks or financial record security. Especially if they require you to provide them with any type of personal financial information, such as social security numbers, account numbers, etc.

4. Take the time to assure your personal electronic devices, such as cell phones, tablets, laptops, and computers, are protected from intrusion. The link below provides you with some guidelines we have published on how to achieve that security.

   https://1919ic.com/wp-content/uploads/2017/08/Mobile-Device-Security.pdf

5. Finally, contact your local law enforcement agency if you think your identity has been stolen or if you believe any of your personal information has been used through this or any other data breach.

At 1919ic we take the security of your information seriously, and take many precautions with the use and dissemination of personal and financial information data. These precautions include:

1. Wire Transfers – 1919ic requires written documentation for all outbound wire transfers that are to an account which is not in the name of the client. If such a wire is requested by email, we require verbal consent from the client prior to wiring the funds.

2. Client Emails – We require any email communication from 1919ic to a client containing personal or financial related information be sent via an encrypted email. Such emails can only be opened by the user who must establish an ID and password for the encrypted email system. Encrypted emails are far more secure than sending password protected files over unencrypted email.

3. Online Access – Access to your 1919ic account through our online portal is done via a secure website requiring dual-factor authentication upon the initial login and any attempt to login through a new computer. This online portal also enables us to securely upload and store client statements and other sensitive documents using advanced encryption technology.

Please feel free to contact us if you would like us to provide more detail on how we protect your information. We will continue to monitor this situation and update you on any significant developments.