THE PORTFOLIO STRATEGY GROUP, LLC

81 MAIN STREET
SUITE 201
WHITE PLAINS, NEW YORK 10601

TEL: (914) 328-6660
(800) 535-5110

FAX: (914) 328-6670

Dear Client,

As you have likely seen, Equifax (one of the three main credit bureaus) had a large security breach that lasted from mid-May through July. There are a lot of notices and alerts suggesting what you can do to protect yourself, so we wanted to share our thoughts with you regarding proactive measures you might consider taking to protect your personal information.

1. Freeze your Credit: Each credit bureau allows you the option to freeze your credit, which helps prevent criminals from being able to open new accounts with your information. You can do this online or via phone, but will need to do so directly through the Credit Bureaus. Please be aware that once your credit is frozen, you will have to un-freeze it before applying for any new lines of credit.

   Equifax:
   - https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp
   - 1-800-349-9960

   Experian:
   - https://www.experian.com/freeze/center.html
   - 1-888-397-3742

   TransUnion:
   - https://freeze.transunion.com/sf/securityFreeze/landingPage.jsp
   - 1-888-909-8872

2. Opt-Out of Prescreened Credit Offers: You likely have received numerous mailings from credit card companies trying to persuade you to open new credit cards. You can stop this by visiting this website https://www.optoutprescreen.com/?rf=t or calling this number 1-888-567-8688.

3. Check your Annual Credit Report: Each of the three bureaus allow you one free credit report check per year by visiting this website https://www.annualcreditreport.com/index.action. It is important to check this at least once per year to see if you notice any suspicious accounts or activity.

4. Update Passwords: Change your passwords on a regular basis and make them with a variety of at least 12 unique characters that would be difficult to crack. There was a good quote given from BNY Mellon's security team, "if the password you choose is in the dictionary, it can easily be cracked."

5. Phishing attacks by e-mail (https://en.wikipedia.org/wiki/Phishing) requesting you or those around you, to do something, are a major risk. PSG will not send you an unexpected e-mail requesting you to explicitly click on a link, read a document or enter personal details. In general, clicking links in any e-mail, even apparently from someone you know, is a risk. Instead, go directly to your browser and use a known web site address.

6. Never email sensitive information such as social security numbers, bank statements, tax returns, etc., unless encrypted.

Our firm is constantly reviewing data security in light of emerging cybersecurity threats, through product enhancements, process reviews and expert input.

If you have any questions about this hack or want to discuss some of the ideas listed above further, please let us know.

Thank you,

The Portfolio Strategy Group, LLC