The following is provided by Calamos Wealth Management to our clients as an informative response to recent high-profile cyber security breaches. We understand that our clients’ financial lives expand beyond our firm and therefore, we want to provide suggestions that promote personal security wherever information is shared and potentially compromised. For specific security measures pertaining to your situation, please consult security professionals where your accounts and information are held.

7 Tips to Protect Your Identity

Please remember to contact Calamos Wealth Management LLC, in writing, if there are any changes in your personal/financial situation or investment objectives for the purpose of reviewing/evaluating/revising our previous recommendations and/or services, or if you want to impose, add, to modify any reasonable restrictions to our investment advisory services, or if you wish to direct that Calamos Wealth Management LLC to effect any specific transactions for your account. A copy of our current written disclosure statement discussing our advisory services and fees continues to remain available upon request.
7 Tips to Protect Your Identity.

While the headlines on high profile information security breaches are becoming more common, they serve to underscore the importance of taking measures to keep your personal information secure. The following provides a few recommendations for you to be vigilant in securing and monitoring your private information and financial accounts:

1. **Check your Credit Report**: Review your credit history. Every person is entitled to a free credit report annually at www.annualcreditreport.com. We suggest you run this report every three to six months. While only one report annually is free, the fee charged for additional reports could be a worthwhile investment.

2. **Set Up Fraud Alerts**: When establishing credit, companies typically run a credit background check with one of the three consumer reporting agencies. Fraud alerts, which last for 90 days, require the companies verify your identity before opening the account. To set a fraud alert, contact one of the companies (see #6 for contact information). That company will then set the alert up with all three. You will have to renew the fraud alert after the initial 90-day time period.

3. **Set Up Alerts with your Financial Institutions**: Enable text or e-mail alerts with your banking, credit card and other financial institutions. These alerts will notify you of transactions on your accounts.

4. **Strong Passwords**: We highly recommend the use of strong passwords and a password manager. Password managers work in conjunction with your smartphone, computer or tablet in generating complex and encrypted passwords. They also help to eliminate some of the common mistakes made in using the same and/or weak passwords.

5. **Enable Two-Factor Authentication**: Financial service firms, e-mail providers, social media sites and others are implementing this technology, which utilizes your normal password, along with a second code that is automatically generated and texted or e-mailed to you. Websites are also beginning to incorporate biometrics (fingerprint and/or facial recognition) to make use of this technology easier.

6. **To Freeze or Not to Freeze**: Consumers who discover their data may have been compromised often inquire as to whether they should implement a credit freeze on their accounts. A credit freeze will not prevent fraud from occurring on existing accounts. A credit freeze restricts access to your credit reports going forward, thereby eliminating the release of your personal information. This is a good proactive step; in order to implement this, you will need to contact each of the three credit providers independently.

   - Equifax: (888) 766-0008
   - Experian: (888) 397-3742
   - TransUnion: (800) 680-7289

However, if you are planning any major purchases, you will need to temporarily "lift" your credit freeze. Typically, the credit reporting agencies will charge a fee for doing so, and it may take a few days to have the credit freeze lifted. Once temporarily lifted, you will need to re-contact the credit providers to re-initiate the credit freeze.

7. **Updated Software**: In addition to the above recommendations, make sure the software on your phone, computer and tablet is updated to the most recent version. Software and hardware manufacturers are always updating and improving the security of their devices. Install and use antivirus and malware software, as well, and never click on a link in an e-mail or text unless you are sure of whom the sender is.
The following is provided by Calamos Wealth Management to our clients as an informative response to recent high-profile cyber security breaches. We understand that our clients’ financial lives expand beyond our firm and therefore, we want to provide suggestions that promote personal security wherever information is shared and potentially compromised. For specific security measures pertaining to your situation, please consult security professionals where your accounts and information are held.