September 14, 2017

SPECIAL ALERT NEWSLETTER

Dear Client,

I wanted to reserve this week's conference call for wrapping up some of the discussions from our annual meeting and to throw some light on what is currently going on in the investing environment. There wasn't enough time to address the Equifax hacking situation during the call, but I would like to address it now and give you some opinions and tips to look out for.

The Equifax hacking is just another example of how inadequate security procedures have been with some of the largest companies. We have all heard about the hacking at companies such as Sony and the Office of Personnel Management (OPM) at the Federal Government. This is happening all too often and I am afraid it will occur even more.

The hack into Equifax is especially disturbing because it affects over 143 million people in the U.S. In other words, I am of the opinion that almost every adult in the U.S has his or her information at risk. This is serious stuff because it isn't a one-time event, but could go on for years. Therefore, I think it would be helpful to offer some advice that I think could be of importance to all of us:

1. I think it is important that you set up some sort of an alert system. My recommendation would be to use Experian's ProtectMyID. Since my personal information was hacked at UCLA and OPM (I am a forest service volunteer) my information was compromised. Both UCLA and OPM gave me two years of free credit monitoring. ProtectMyID only alerts you when someone is inquiring or asking for credit on your behalf. For most people, this is sufficient enough. However, for related details, you might have to buy a credit report for $31. Although the State of California mandates that one credit report is given free each year, this service provides the full credit reports from Equifax, Transunion and Experian all in one convenient report. Personally, since I was hacked at UCLA and OPM, I buy the report twice a year to see what is going on with my credit. I think this is cheap insurance and well worth the cost. If you are eligible for the free service from ProtectMy ID, that's great, but even if you have to pay for it, it is worth it.

2. You might want to consider freezing your credit. With the recent hacking, someone can apply for credit under your name. The downside is that your credit is locked and if you apply for a new credit card, line of credit, or home loan, it is a pain to unlock. In order to successfully lock and unlock your credit, you need to lock and unlock it with Experian, Equifax and Transunion. Not one credit rating agency but *all* three. Since I personally don't anticipate using any additional credit at this time, I am considering freezing my credit. I would think this over carefully and wait a few weeks before I would contact the credit agencies. Let the dust settle before you call due to millions of people overwhelming the credit agencies' phone lines. Do not mail any personal information requesting a credit freeze because all of your personal information could be stolen through the mail system. The U.S. mail is not trustworthy enough for you to mail all of your personal information.

3. If you have been hacked, hackers have your social security number. These creeps could apply for any tax refunds generated from your income tax filings. A suggestion here would be not to request a tax refund but apply any overpayment to your future taxes. Tax refund fraud has been a

huge problem with the IRS costing taxpayers billions of dollars as people request tax refunds under social security numbers besides their own. Hackers might try to apply for tax refunds so it is advisable to file your tax return as early as possible before April 15th.

4. Carefully review your credit card statements and don't use debit cards. If there is a charge on your credit card statement that you didn't purchase, the credit card company will have to eat the charge, not you. Not so with debit cards so don't use them.

5. If you have multiple financial accounts that are linked together, change passwords on each account and make sure your password is strong. Don't use birthdates, anniversaries, social security numbers or phone numbers.

6. Last year, we wrote to all of our clients that we will not send out any wire without a verbal confirmation. At the time, we felt that this was a necessary security precaution and I feel even more strongly about it now. Fidelity has sophisticated signature recognition technology in which your signature has to exactly match what Fidelity has on file. We have tested the system by submitting a phony signature and the wire did not go through, Fidelity called us. If you need money from your accounts, please call us and we will safely and securely process your request. I am confident that your money is safe at Fidelity. We get alerts each day on all account activity so we are able to monitor your Fidelity accounts. We would know of any suspicious activity at any time.

With the support of Super Source Consulting we have been upgrading our cybersecurity and our computer system. We feel confident that it is secure but we will continue to invest in keeping our computer network safe and secure.

If you have any questions, please feel to call me. I hope this special newsletter is helpful.

Sincerely,

Steve Yamshon
Investment Counsel