The brave new, digital world that we all live in continues to be a risky place. The recent revelation that one of the three large credit reporting firms, Equifax, was itself the victim of a security breach that exposed sensitive information for 143 million Americans feels particularly disheartening. Most people today seem to wonder if their data has been breached and exposed.

The raw number of exposed citizens is astounding with 143 million roughly equal to the number of employed Americans. If you exclude children from the population count, this would suggest that more than half of us are at some risk of identity theft from this incident alone. Given the magnitude of this breach, we wanted to share with you some suggestions about how you can protect yourself in the coming months.

The single most important step is to remain vigilant. There is simply no substitute for your attention to your own affairs. This means that bank and credit card statements need to be carefully reviewed and reconciled. You should also review your investment statements from Schwab and any other custodian that you have. If something seems out of order, follow up and ask questions of the institution. You should also review your credit report annually. You can request a free report each year from the credit agencies, or you can request a copy from www.annualcreditreport.com.

If you believe that you have been the victim of identity theft or want to learn more, you can contact the Identity Theft Resource Center at 888-400-5530 or www.idtheftcenter.org.

While the imperative to be vigilant always applies, there are some specific steps that you may consider now:

Security or Credit Freezes

The most dramatic step that you can take is to initiate a credit freeze. This involves contacting each of the three major credit firms and freezing your account. This will prevent anyone from opening a credit instrument in the name of the consumer. If you are not anticipating taking out any new credit (i.e., getting a new charge account, mortgage, car loan or credit card), this probably makes sense. If circumstances change, you will need to remove the freeze by contacting the three credit agencies again but this should be a relatively easy process. Contact information is as follows:

Equifax: 800-349-9960 or visit its website https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp#

Experian: 888-397-3742 or visit its website https://www.experian.com/freeze/center.html

Transunion: 888-909-8872 or visit its website https://www.transunion.com/credit-freeze/place-credit-freeze

It is important to note that this step will **not** impact current credit cards or financial accounts. It does not eliminate the need for your vigilance, and it does not mean that you cannot have invalid charges appear on your credit cards.

Fraud Alerts

You can also contact the credit agencies and establish fraud alerts. These alerts will not freeze your credit, but will instead notify you if there is a credit inquiry. They generally last 90 days but are renewable. Longer periods of alerts are available at no cost if you are the victim of identity theft as demonstrated by a report filed with a law enforcement agency.

If you opt not to freeze your credit, there is little downside to these notifications.

Credit Monitoring

Credit monitoring is designed to offer the fraud alert services along with reviews of any other suspicious activities. They generally carry monthly or annual charges and are available from firms including Lifelock, Identify Guard and myFICO. Equifax is offering the service for a year for free if you sign up prior to November 21, 2017. Some critics suggest that this may a case of the fox keeping an eye on the henhouse, and if you agree you may be more inclined to the private offerings.

The Equifax offering can be established at a new website: www.equifaxsecurity2017.com.

Other Best Practices

As always, use strong and regularly updated passwords at any website that you visit. If you make online purchases and have multiple credit cards, consider dedicating one card with relatively modest credit limit for online activity only (and watch those card statements closely). *And, perhaps most importantly,* ***NEVER EVER*** *respond to any via email, mail or phone for your personal or financial information.* Your bank, credit card companies, utilities, asset custodians and the IRS do not contact you via phone or email and request or demand your information. If you have business to conduct, you should make an outbound call or contact to the entity or institution.

We take your information privacy and security very seriously and look forward to continuing to work together to protect you from cyber-crime.