Securing Your Personal Data in an Insecure Cyber World

By now, most people have heard of the Equifax data breach, which affects the accounts of more than half the adult population of the United States. Because October is "National Security Awareness Month," we would like to offer some thoughts and suggestions as to what steps you might take in light of the Equifax data breach.

1. **Assume your data has been disclosed. Equifax has a website where you can check to determine if your personal data has been disclosed. The problem has been that the response is not reliable. For example, in my own situation, one time the website told me my data had been disclosed, and another time the website told me my data had not been disclosed. Therefore, it is safer to assume your data has been disclosed, even if it means you might end up with some extra aggravation and expense.**

Note: Early rumors that, by using the website, you are waiving your rights against Equifax, are incorrect.

2. **Monitor Your Accounts. Monitor your existing credit accounts for suspicious transactions. Each of the 3 major credit reporting companies (Equifax,Experian and Transunion) will provide one free report per year. You may want to stagger those to obtain one from a different vendor every four months. Look for new accounts in your name.**

Alternatively, you may want to sign up for free credit monitoring service. Equifax is offering a free credit monitoring service to holders of U.S. social security numbers, if you sign up by January 31, 2018. If you are uncomfortable with Equifax monitoring your credit, you may sign up with an independent monitoring service, but there may be a fee.

Again, an early rumor that Equifax's credit monitoring terms and conditions require you to give up certain legal rights has turned out to be false.

3. Consider a Fraud Alert or Credit Freeze. You should also consider placing a fraud alert on your file with the three credit report companies. This is a renewable, 90-day alert that requires lenders to verify your identity before issuing credit. This fraud alert should make it more difficult for someone to open new accounts in your name without your knowledge.

Some advisors are recommending that you place a "credit freeze" on your file with the three credit report companies.

The benefit of the credit freeze is that it prevents anyone, including you, from obtaining new credit in your name. One disadvantage is that, depending on the state where you live, there may be a fee each time you place or remove the credit freeze. For example, Rhode Island residents must pay a $10 fee, and Massachusetts residents must pay a $5 fee, unless you are over 65 or you are actually the victim of identity theft and provide a copy of a police report. Another inconvenience with a credit freeze is that the freeze also stops you from obtaining new credit. If you want to apply for a new credit card or a new car or mortgage loan, you will need to contact each of the credit reporting companies, and possibly pay a fee, for a temporary lift of the freeze.

4. Watch out for phishing attacks. Be very careful of emails you may receive regarding the Equifax breach, both at work and at home. These emails may be sophisticated, and ask you to click on a link or button and provide personal information. DO NOT CLICK ON THEM OR PROVIDE PERSONAL INFORMATION. Neither Equifax, or your Bank, or Consumer Reports, or your investment broker, or the IRS, or anyone else is going to request personal information from you online.

5. **Watch Your Mail. Monitor your mail for changes. Does the volume seem lower? Did you not get mail for a day or two? Because credit card companies mail out new cards, scammers will apply for credit in your**

name, but with a different address. Then they will change your mailing address with the United States Postal Service to forward the mail to the new address, so they receive the new credit card.

6. Check Your Investments. Investment firms, unlike banks, are not required to restore assets stolen by hackers. Check with your retirement plan or 401(k) plan administration or your investment broker to determine whether or not they have a policy in place to reimburse funds taken by a hacker, and whether the policy requires you to take any affirmative action (enrollment, up-to-date antivirus software in your computer, etc.)

Many of us have also been affected. It is normal to feel angry or frustrated. But it is even more frustrating to have someone open a credit card or account or borrow money in your name. By taking some of these steps, you will have reduced your cyber risk significantly.

Date Created
October 4, 2017