In the Wake of the Equifax Breach, Steps to Protect Yourself From Identify Theft

Equifax, one of the largest credit monitoring and reporting agencies in the US, is one of the latest companies to fall victim to an online cyber security breach, putting nearly half of the US populations' personal information including names, dates of birth, social security numbers and drivers' license information, at risk. Does the Equifax breach impact you? It depends on a variety of factors, but unfortunately, it is likely that the answer is yes.

What does this mean?
The Equifax data breach means that someone with access to your personal identifying information, such as your DOB (date of birth) and SSN (Social Security Number) could open new lines of credit, take out loans, and even file for a fraudulent tax refund in your name.

What can be done?
To protect yourself from becoming a victim of identity theft and to regain control over your financial and personal information, start with these steps:

1. Be aware that although your personal information may have been breached, it does not mean that you are a victim of identity theft. **Identity theft** occurs when someone else uses your personal information to obtain credit, loans or other benefits in your name without your knowledge or consent.

2. To see if your personal information has been impacted, check Equifax's special website where you can find out if you were one of the 143 million individuals impacted. Upon entering some basic information, you may receive a message stating, "We believe your personal information may have been impacted by this incident" and then a link to enroll in free credit monitoring services.

    - The credit monitoring service is being offered for free to individuals who may have been impacted by this cyber security breach. The first year of service is being provided for free, but at present, you only have until **Tuesday, November 21, 2017,** to enroll for these services.
    - The service will provide you with credit monitoring services from three national credit reporting agencies: Experian, TransUnion and Equifax.

- It will lock your credit file – but only with Equifax (see below for more information on how to freeze your credit file with the other two credit reporting agencies).
- It will provide you with SSN monitoring services and identity theft insurance.
- At present, there seems to be some concern about accepting this free credit monitoring service and forfeiting your rights to seek legal action outside of mandatory arbitration. However, according to Equifax's Terms of Use for TrustedID Premier, as of September 8, 2017, there are no mandatory arbitration clauses.

3. You should also **check your credit report** with all three credit reporting agencies to see if there is any unusual activity on your credit file or unauthorized accounts being opened. You can obtain a free annual report from each of the agencies by visiting https://www.annualcreditreport.com.

    - If you do see suspicious activity on any of your accounts then you should dispute the information by following the instructions provided by each of the Credit Reporting Agencies.

4. Consider placing a **fraud alert** on your credit file. A fraud alert puts a notice on your credit file which lets creditors know that your identity needs to be verified before a new line of credit is issued. There is no fee to place a fraud alert on your credit file, however, you must notify each of the credit reporting agencies. This may be done online, by mail or by phone. See each of the agencies' web pages for specific information (Experian: www.experian.com; TransUnion: www.transunion.com and Equifax: www.equifax.com).

    - There are 3 types of fraud alerts:
        1. 90 day Fraud Alert: Lasts only 90 days and can be obtained by anyone 18yrs or older
        2. Military Fraud Alert: Lasts for one year, but can be extended to the full term of deployment
        3. 7 year Fraud Alert: Can be obtained by victims of identity theft and requires you to have a police report or an FTC Identity Theft Report.

5. Consider placing a **credit freeze** on your credit file. A credit freeze is the most comprehensive form of protection. A credit freeze will prevent any new lines of credit from being opened as well as prevent inquiries into your account. To obtain a credit freeze, you must contact each of the credit reporting agencies.

    - A credit freeze is free if you are a victim of identity theft and have a police report or an FTC Identity Theft Report. Once you have a credit

freeze on your credit file, if you choose to apply for a new line of credit, you will need to lift the freeze. It may take a few days for each agency to process the information and there may be fees associated with this process.

6. If your Social Security Number has been breached then you should also be on the lookout for tax-related identity theft, which may be the result of fraudulent tax filings. The IRS has more information on what to do if you suspect you are a victim of tax-related identity theft on their website.

It is crucial to take the necessary steps and act now to protect your financial and personal information. Whether or not you decide to enroll in the free credit monitoring services offered by Equifax, or place a credit freeze or fraud alerts on your credit accounts, you should be checking your credit reports regularly. Following at least one of these steps could prevent you from falling victim to identity theft and will help you feel more in control of your privacy and confidential information.

For other helpful online resources, please see the links below:

- Federal Trade Commission's (FTC) website for consumers has the latest news on phone and email scams. They also have a separate website with information on what to do when you are a victim of identity theft. This website also gives you access to their FTC Identity Theft Report, which can be used to obtain specific fraud alerts and credit freezes without charge.
- Identity Theft Resource Center provides sample letters to credit reporting agencies and information on your rights as a victim of identity theft.