PATRIOT INVESTMENT MANAGEMENT

The Equifax Data Breach and What It Means to You

What Happened

One of the "Big Three" credit bureaus, Equifax's databases were hacked sometime in mid-May, exposing consumers' personal data, including Social Security numbers, home addresses, credit card numbers and birthdates. Equifax found the intrusion on July 29th, but did not disclose it to the public until September. This is one of the largest data breaches in history, with 143 million consumers affected, or roughly half the US population.

In response, Equifax is offering one free year of credit monitoring (after which you will be charged a fee for the service), and has set up a website for consumers to check if their personal data was compromised. However, the site seems to be broken, often returning different results for the same data submitted at different times. In addition, it was found that their mobile apps were not secure; Equifax has since removed them from Apple's App Store and Google Play. An investigation of the data breach and Equifax's response to it are ongoing, so expect to see more news over the coming weeks and months ahead.

What You Can Do to Protect Yourself

Less talked about is the fact that this is not the first time that a credit bureau or even Equifax had had consumer data compromised. Given the size of this data breach, as well as past intrusions at Anthem Insurance, the Office of Personnel Management (OPM), Home Depot, Target and many others, it is best to assume your data has been compromised at some point along the way.

1. **Enroll in a credit monitoring program (optional) –** Signing up for credit monitoring can't hurt, but be aware that it **cannot prevent identity theft.** Ideally, the service will notify you when an identity thief has stolen your identity, so that you are able to more quickly respond once the theft has occurred. There are several companies that offer credit monitoring, such as AllClearID and LifeLock, which was acquired by Symantec earlier this year. Using a credit monitoring service is not enough, and can provide a false sense of security.

2. **Freeze your credit –** The single best thing you can do to prevent your data being stolen in the first place is to file a credit freeze – also known as a security freeze – with the four largest credit bureaus (Innovis is the fourth largest), and ChexSystems, which provides credit data verification for banks opening checking and savings accounts. (Experian and TransUnion are the other two). A credit freeze blocks your credit file from being pulled by creditors. You will have a PIN for each bureau, which you can use to temporarily lift the freeze for legitimate creditors, such as applying for a mortgage or auto loan.

The set-up cost ranges from free to $15 per bureau, depending on your state. In Tennessee, setting up a credit freeze is $7.50 per bureau, and free for minors and ID theft victims; it is also free to temporarily lift the freeze. While there is a cost to freezing your credit, it is typically less than what you will spend on credit monitoring, and with better protection. If you choose to also do credit monitoring, sign up for it first, as the freeze will prevent enrollment once it is in place. Consumers Union has a breakdown of state-by-state fees.

Setting up a freeze can be done online or over the phone:

Equifax: 1-800-349-9960

Experian: 1-888-397-3742

TransUnion: 1-888-909-8872

Innovis: 1-800-540-2505

ChexSystems: 1-800-887-7652

3. **Request your credit report –** By law, you can pull your own credit report annually, for free, from each of the three major bureaus, available at www.annualcreditreport.com. Review carefully for any accounts you don't recognize, late payments, etc., and alert the credit bureaus if you find evidence of ID theft.

4. **Request a fraud alert –** A fraud alert can be placed on your file for free; however, it is only good for 90 days, after which you will need to renew it. With one in place, the credit bureau should contact you if someone tries to apply for credit in your name, but they are under no legal obligation to do so. Fraud alerts are not the same thing as a credit freeze or credit monitoring, and, used by itself, can also cause a false sense of security. Taken together, these three tools are the best way you can protect yourself.

5. **Repeat for loved ones –** Follow steps 1-4 for family members, including minors, if allowed in your state. The National Conference of State Legislatures has a state-by-state listing for freezing children's accounts.

Other useful links:

California's Department of Justice has the most comprehensive list of companies who have had data breaches; although not exhaustive: https://oag.ca.gov/privacy/databreach/list

The Federal Trade Commission's guide to child identity theft: https://www.consumer.ftc.gov/articles/0040-child-identity-theft

Identity Theft Resource Center: http://www.idtheftcenter.org/