What Should I Do About the Massive Data Breach at Equifax?

9/8/17

By Rohit Chopra, Senior Fellow, Consumer Federation of America

Yesterday, Equifax revealed that a data breach has impacted approximately 143 million American consumers. Names, addresses, Social Security numbers, birth dates, and driver’s license numbers were accessed. Hundreds of thousands of consumers also had their credit card numbers exposed.

If you haven’t heard of Equifax, it’s one of three major consumer credit reporting agencies along with TransUnion and Experian. Banks and other financial companies report information about you to these companies. They use this data to market financial products to you and to make decisions about loans. Employers and landlords also look at credit reports to determine whether to offer you a job or an apartment lease.

In recent years, the Consumer Financial Protection Bureau and Federal Trade Commission settled charges of unlawful conduct with Equifax, TransUnion, and Experian that led to restitution and penalties. But requirements on what a company must do after a data breach are generally governed by state law. Most states require notifications to victims, but some states offer other protections.

The company has established a website about the breach. If you want to check if data about you was accessed, you must enter the last six digits of your Social Security number. Many consumers may be wary of providing this information given this massive breach.

Equifax also established a call center to help answer questions about the situation. It seems like volume is heavy: I called twice this morning and got a hang up and a busy signal.

The situation is evolving, and hopefully we will learn more soon, but many people are
wondering: what can I do now?

Consider a security freeze.

The best protection from many types of identity theft that can result from data breaches is to activate a security freeze. If you put a freeze on your credit file, prospective lenders, landlords, or employers won’t be able to access your credit report. If you – or a criminal – applies for a loan with your information, the lender will deny the application.

If you choose this route, you’ll need to contact each of the three major credit reporting agencies, not just Equifax. Learn more here.

Get a copy of your free credit report.

Federal law allows you to get a free copy of your credit report each year. If you haven’t checked them this year, I would recommend you check your reports from Experian and TransUnion. Consider checking one of them now and the other in a few months. Don’t pay to get your credit report! Learn more about your rights here.

Scan through your credit report to see if there any new accounts that may have been recently opened without your authorization.

Check your credit card bills closely.

Equifax has stated that it will contact consumers if their credit card information was compromised by sending them a notice in the mail. Don’t wait for this.

When you log into your online account for your credit card, comb through each transaction to
see if anything looks suspicious. If you haven’t lost your card, but your credit card number was used without your authorization, you won’t be liable. You should report the suspicious transactions immediately to your credit card company. They’ll likely re-issue you a new credit card.

*Be extra careful about incoming offers and suspicious e-mail links.*

With so much of your personal information compromised, scammers might be able to target you with the goal of extracting more information out of you that could be misused. Never click on suspicious links and avoid providing additional personal information unless you can verify who is asking for it and why it is needed.

*Protect your e-mail account.*

Many websites allow you to change your password when you type in personal information, like a Social Security Number. Usually, these websites e-mail you a link where you can then change your password. If a hacker is able to access your e-mail account, they can potentially do much more damage, changing passwords for many of your other accounts.

Consider strengthening your password for your e-mail account. Many commercial providers now offer “two-factor authentication,” where you receive a phone call or text message with a secret code that must be entered before your account can be accessed from a new device. Enable this.

Bottom line: carve out an hour to protect yourself and your family. Even if your information wasn’t stolen, you’ll be better prepared for the next cyberattack.