The Equifax Data Breach: What to Do

September 8, 2017
by Seena Gressin
Attorney, Division of Consumer & Business Education, FTC

If you have a credit report, there's a good chance that you're one of the 143 million American consumers whose sensitive personal information was exposed in a data breach at Equifax, one of the nation's three major credit reporting agencies.

Here are the facts, according to Equifax. The breach lasted from mid-May through July. The hackers accessed people's names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. They also stole credit card numbers for about 209,000 people and dispute documents with personal identifying information for about 182,000 people. And they grabbed personal information of people in the UK and Canada too.

There are steps to take to help protect your information from being misused. Visit Equifax's website, www.equifaxsecurity2017.com. (This link takes you away from our site. Equifaxsecurity2017.com is not controlled by the FTC.)

- Find out if your information was exposed. Click on the "Potential Impact" tab and enter your last name and the last six digits of your Social Security number. Your Social Security number is sensitive information, so make sure you're on a secure computer and an encrypted network connection any time you enter it. The site will tell you if you've been affected by this breach.
- Whether or not your information was exposed, U.S. consumers can get a year of free credit monitoring and other services. The site will give you a date when you can come back to enroll. Write down the date and come back to the site and click "Enroll" on that date. You have until November 21, 2017 to enroll.
- You also can access frequently asked questions at the site.

Here are some other steps to take to help protect yourself after a data breach:

- **Check your credit reports** from Equifax, Experian, and TransUnion — for free — by visiting annualcreditreport.com. Accounts or activity that you don't recognize could indicate identity theft. Visit IdentityTheft.gov to find out what to do.
- **Consider placing a credit freeze on your files.** A credit freeze makes it harder for someone to open a new account in your name. Keep in mind that a credit freeze won't prevent a thief from making charges to your existing accounts.
- **Monitor your existing credit card and bank accounts closely** for charges you don't recognize.
- If you decide against a credit freeze, **consider placing a fraud alert on your files.** A fraud alert warns creditors that you may be an identity theft victim and that they should verify that anyone seeking credit in your name really is you.
- **File your taxes early** — as soon as you have the tax information you need, before a scammer can. Tax identity theft happens when someone uses your Social Security number to get a tax refund or a job. Respond right away to letters from the IRS.

Visit Identitytheft.gov/databreach to learn more about protecting yourself after a data breach.