The Equifax breach and you: be proactive

Earlier this year, hackers were able to breach the security of Equifax, one of the three national credit reporting agencies. More than 143 million Americans – nearly half the entire country – were exposed to the attack, and may have had their personal information stolen (including names and birthdates, and Social Security and driver's license numbers).

Equifax is still determining exactly whose data has been exposed. While you wait to find out, it's worth taking a few proactive steps to make sure your info isn't misused by hackers.

1. Start checking. Visit Equifax's website at www.equifaxsecurity2017.com and enter your last name and last six digits of your Social Security number. The site will tell you whether it's likely or not your data has been exposed, and put you on a list to get more information. You can also sign up for a year's worth of free credit monitoring.

2. Watch your statements. Start checking your credit card statements, and pay special attention to cards you don't use often. The initial reports from the breach were that hackers may have been making charges on underused cards.

3. Check your credit reports. You can look for suspicious items on your reports, such as new accounts being opened in your name, at all three credit report agencies: Equifax, Experian and TransUnion. Free annual reports are available at www.annualcreditreport.com. You may want to stagger your use of the reports to one from each agency every four months. More frequent checks will cost you a small fee.

4. Freeze your credit. If you suspect you may become a victim of identity theft, you can place a credit freeze on your profile at each of the three credit reporting agencies. This stops new accounts from being opened in your name. Note that you'll have to unfreeze your accounts if you want to apply for new loans or make your credit accessible for things such as job applications.

5. File your taxes early. One of the most common ways identity thieves use your information is to try to claim a tax refund with your data. This was the most common scam in 2016, according to the Better Business Bureau. If you file your tax return as early as possible, you shut down this opportunity for any would-be thieves.