Steps to Help Protect Your Identity Following the Equifax Data Breach

Equifax has announced that cybercriminals have exploited a vulnerability in their website, allowing them to gain access to certain files. The data breach appears to have taken place from mid-May through July 2017. The company discovered the unauthorized access on July 29 of this year.

Cybercriminals stole names, Social Security numbers, birth dates and addresses. In some cases, driver's license numbers and even credit card numbers were accessed. During the company's investigation of this breach, it was also found that there was access to some personal information for some UK and Canadian residents.

How do you know if you have been involved in a data breach?

Usually, data breaches are disclosed via the company's press release, which reaches news outlets in no time. If you hear about a breach involving an institution you do business with, contact the organization in question to check whether your data has been compromised. You can visit the organization's website to see if there is a statement about the breach with any instructions about what to do next, or you can call the company's customer service phone number.

Helping protect yourself in the event of a data breach

You may not know if you have been affected by a breach, so your best action is to be proactive. You can use the tips below to stay ahead of the bad guys and know what to look out for.

- Routinely monitor all of your financial accounts for suspicious activities, such as transactions you did not make. If your institution offers account activity alerts via text or email, sign up for them.
- Cybercriminals can now use these data to access other online accounts you may have via password reset questions. These questions usually ask you personal information about yourself such as a parent's maiden name, previous addresses and other details. If you have used any of these data in those security questions, you should change those questions immediately.
- If the information that was leaked in the breach was a Social Security number or other personally identifiable information, you may want to consider putting a security freeze on your credit report. This will prevent other institutions from accessing your report entirely, which will prevent opening any new credit lines or credit extensions under your name. Also be sure to contact the Social Security Administration about next steps if you're dealing with a data breach that involves your SSN.
- If you do encounter suspicious activity on your account, contact your bank immediately and inform them of the activity as well as the fact that your information was exposed in

a breach. Secondly, contact the FBI's Internet Crime Complaint Center (IC3) and file a report.
- If a password was involved in the breach, change it.

These are just a few of the precautions one can take to help protect against identity theft.

Breaches are more common these days, and the payoff for cybercriminals may be lucrative. As a result, it can be helpful if you add another layer of protection to your digital life by using an identity theft protection service. Such services can help protect your personal information by sending you alerts if suspicious activity is identified within their network, or if new accounts are opened with your Social Security number†.

This article is authored by an employee of Norton by Symantec.

No one can prevent all identity theft.

† LifeLock does not monitor all transactions at all businesses.

* Credit card required at enrollment. At the end of the no-cost 30-day trial period, if you do not cancel, your card will be billed automatically on a monthly or annual basis depending on what you elect at the time of enrollment. Offer is for new LifeLock members only. Offer is available for LifeLock Standard™, LifeLock Advantage™ and LifeLock Ultimate Plus™ memberships only. Not combinable with other offers.