How to Respond to a Data Breach

You may have read that hackers broke into the Equifax database and stole personal information tied to 143 million people. 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. There is no reason to think that data is not for sale to criminals who can use it to open new lines of credit or file phony tax refund requests in peoples' names.

The company compounded its public relations nightmare by sending people to a website to find out if they were affected, and then including language so that anyone signing in to get this information had to waive any right to join a class action suit against the company should their identities be stolen and financial harm come to them.

The negative publicity forced Equifax to delete the waiver, but when you sign into the web page to find out if you were affected (the link is here: https://trustedidpremier.com/eligibility/eligibility.html), the site requests the last six digits of each person' social security number—and guessing first three isn't as hard as you might think since different regions of the country use pre-assigned digits. If you're still worried about Equifax's data security, then the company's request for additional personal information is worrisome.

If you have credit, then there's a high probability that identity thieves now have your Social Security number and address. To contain the potential damage, the U.S. Federal Trade Commission recommends that you take several steps immediately. First, under federal law you're allowed to request a free copy of your credit report once a year from each of the three credit reporting agencies: Equifax, Experian, and TransUnion—at www.annualcreditreport.com. You can do this every 122 days by rotating among the agencies. Look for suspicious accounts or activity that you don't recognize—such as someone trying to open a new credit card or apply for a loan in your name. If you DO see something, visit http://www.Identitytheft.gov/databreach to find out how to mitigate the damage.

Then monitor your online statements. The credit report won't tell you if there's been money stolen from a bank account or suspicious activity on your credit card. Unfortunately, you'll have to turn this into a habit. In most cases, theft happens over time, starting with small amounts stolen from across your accounts.

Finally, place a credit freeze and/or fraud alert on your account with all the major credit bureaus. You can put a fraud alert, for free, by contacting one of the credit agencies, which is required to notify the other two. This will warn creditors that you may be an identity theft victim, and they should verify that anyone seeking credit in your name is really you. The fraud alert will last for 90 days and can be renewed.

If you're really worried, consider putting a freeze on your credit.

A freeze blocks anyone from accessing your credit reports without your permission—including you. This can usually be done online, and each bureau will provide a unique personal identification number that you can use to "thaw" your credit file in the event that you need to apply for new lines of credit sometime in the future. Another advantage: each credit inquiry from a creditor has the potential to lower your credit score, so a freeze helps to protect your score from scammers who file inquiries.

Fees to freeze your account vary by state, but commonly range from $0 to $15 per bureau. You can sometimes get this service for free if you supply a copy of a police report (which you can file and obtain online) or affidavit stating that you believe you are likely to be the victim of identity theft.

Many Americans have opted to sign up for a credit monitoring service, which won't prevent fraud from happening, but WILL alert you when your personal information is being used or requested. In most cases, there is a cost involved, but Equifax is offering a free year of credit monitoring through its TrustedID Premier business, whether or not you've been affected by the hack. It includes identity theft insurance, and it will also scan the Internet for use of your Social Security number—assuming you trust Equifax with this information after the breach.

There's one last way you can protect yourself. ID thieves like to intercept offers of new credit sent via postal mail. If you don't want to receive prescreened offers of credit and insurance, you have two choices: You can opt out of receiving them for five

years by calling toll-free 1-888-5-OPT-OUT (1-888-567-8688) or visiting www.optoutprescreen.com.

Or you can opt out permanently online at www.optoutprescreen.com. To complete your request, you must return a signed Permanent Opt-Out Election form, which will be provided after you initiate your online request.

Sources:

https://www.equifaxsecurity2017.com/potential-impact/

https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do?utm_source=slider

https://krebsonsecurity.com/2015/06/how-i-learned-to-stop-worrying-and-embrace-the-security-freeze/

http://money.cnn.com/2017/09/09/pf/what-to-do-equifax-hack/index.html