Mic

Equifax data breach 2017: 3 smart ways to protect your credit and identity right now — and beyond

Published Sept. 12, 2017

by Christy Rakoczy

Equifax data breach got you stressed out? Don't panic. Here's what to do and know if your information was hacked — including the pros and cons of setting up a fraud alert.

It seems like every day, there's news of a data breach at a major company that puts your information at risk. The recent breach of Equifax data, however, was a little different both because of its massive scope — the majority of U.S. adults were likely affected — and because of the breadth of information hackers could obtain from the records that Equifax has.

You have a few ways to act now. The website DoNotPay has pre-filled the forms to file a small claims court case against Equifax in a limited number of states, including New York and California. At press time, DoNotPay was not working for *Mic*, but Joshua Browder, the service's creator, said in a message that it should be back up later today. (If you pursue this option, you should be aware that you may have to take these pre-filled forms to your local small claims court, pay a filing fee and attend a small claims court hearing.)

How do you keep your data from getting compromised in the first place? Lawmakers are pushing for legislation that would require credit reporting agencies to correctly match names, addresses and social security numbers. That would reduce the chance that your identity gets mixed up with someone else's, which could tank your credit score.

Generally, the best way to protect your personal data and avoid becoming a victim is to be vigilant at all times. "If you take steps in advance of another breach, which will happen, then you will be in pretty decent shape," Nick Sloane, a Chartered Financial Consultant and President of Sloane Wealth Management, said in an email interview.

But if that sounds exhausting — and you need more concrete advice — don't fear. Here are three simple key steps you can take right now.

1. Double down on “normal” safeguards

Your best option is to make sure you’re locking down personally identifying information, and the lucky news is that you can do that through some easy moves — which you should be undertaking in good times and bad anyway.

“If you’re already practicing good identity hygiene, your behavior won’t need to change that much after the breach,” Eva Velasquez, CEO and president of the nonprofit Identity Theft Resource Center said in a phone interview.

What is identity hygiene? It refers to following a few steps on a regular basis to protect your personal data. Velasquez recommended a simple acronym to make it easy to remember the steps to take: SHRED, which stands for:

• **S**trengthen your passwords and privacy settings. Choose passwords only you would know and use unique passwords for sensitive accounts, like your email and bank accounts. It’s also smart to change your passwords every 90 days.

• **H**andle your personal information with care: “The information that makes up your identity is valuable,” Velasquez points out. Yet, people post all kinds of personal information online, even sometimes sharing pictures of their driver’s licenses, for example. Avoid posting pictures of any personal documents and shred mail that has identifying information.

• **R**ead your credit reports regularly: This is different than just checking your credit *score*, which Velasquez says is not enough. Annualcreditreport.com allows you to check each of your reports from the three major credit bureaus — Equifax, Experian and TransUnion — for free once a year. Set a reminder on your calendar to pull one report every four months to keep regular tabs on your credit at no cost.

• **E**mpty your purse and wallet: “People just carry too much info,” Velasquez said. “If you throw everything in your purse or wallet, it’s a treasure trove for thieves.” It’s best to carry as little as possible and avoid carrying highly valuable information — like your social security card.

•**D**iscuss with friends: You should talk with your friends about protecting their own identities, too. Scammers who hack those in your address book could easily find and target you.

In addition to these best practices, it’s also a good idea to check your credit card and bank statements for any weird charges you didn’t make. Using a service like Mint, which collects all of your financial information in one place, could make it easier to check statements for charges you may not have made.

And, remember that it’s not just your credit cards at risk: Thieves can file phony tax returns with your information to claim refunds they aren’t owed and once they’ve filed with your tax return, you’re essentially locked out of doing your own filing. “Someone can beat you to the punch and file a return in your name, with refund checks being sent to them,” Sloane said. To help protect your refund, file your taxes early, before someone unscrupulous uses your info first.

2. Build a wall around your credit

Thieves often steal your identity because they want access to your credit, but you can lock them out by building a wall around your credit. This is actually simple to do through a "freeze," although there might be a cost.

"A credit freeze disallows anyone, including yourself, to try to get credit," Sloane told *Mic*. "Contrary to what some believe, initiating and then doing temporary lift of a freeze is by no means burdensome. Costs of doing this vary state by state. This has no effect on your credit report."

To freeze your credit, contact each of the credit reporting companies and provide your personal identifying information. You can reach the three nationwide credit reporting companies at these numbers:

Equifax — 1-800-685-1111
Experian — 1-888-397-3742
TransUnion — 1-888-909-8872

When you freeze your credit, you'll usually be given a PIN that you can then use to temporarily lift the freeze, Sloane said. "When applying for credit, simply ask which reporting agency they use and you only need to do the short term lift with that company."

Another alternative is to set up a fraud alert, which you'll need to renew every 90 days. TransUnion, Equifax and Experian all let you place a fraud alert. Once you've done so, businesses will always have to verify your identity — usually by contacting you when an application for credit is submitted in your name.

Finally, you should also opt out of prescreened credit offers unless you really want to take advantage of them, according to Sloane. "The reason for this is that mail theft is rampant. The same goes for the free checks you get from your credit card company. Tell them to stop sending checks."

You can also restrict thieves from accessing your mail if you really want to be safe: "If you have an unsecured mail box, consider some kind of locking box at your local post office or a UPS store," Sloane said.

3. Get in vigilance mode

Unfortunately, no matter how careful you are, breaches can still happen. And, once they do, you need to be very careful going forward.

“Whenever we have big events, the scammers will come out with a one-two punch,” Velasquez said. “Watch out for things like shady websites saying they’re part of Equifax consumer services and watch out for people calling or sending text messages for links. Make sure you know who you’re talking to, and go back to the source to confirm that the message is legitimate.”

Thieves can be really convincing if they have your Social Security number and other personal information from the Equifax breach, so keep up-to-date on any scams that are being reported. You can sign up for scam alerts from the Federal Trade Commission to keep tabs on tricks thieves are currently using to target consumers.

Velasquez also recommends making sure to open all mail you receive, especially from companies you do business with. “A lot of people get rid of mail because they think it’s a solicitation, but it could be a company trying to get in touch with you to ask if you opened an account. Take the 30 seconds to open the correspondence to make sure it’s not important.” Again, investing in a good paper shredder could make life easier.

By being vigilant about what’s being done in your name, you can keep yourself safe from loss — even after big data breaches.