



## The Equifax Data Breach: What You Need to Know, What You Can Do

*If you're an adult living in the U.S., there's a better than 50 percent chance your data was stolen.*

Along with TransUnion and Experian, Equifax is one of the three major credit reporting agencies. They track your entire financial history — bills, loans, credit cards and more. They use this info to build your credit report. Even if you've never used an Equifax service, they likely have your information on file.

According to Equifax, hackers breached their system from mid-May through July 2017. Hackers got the names, Social Security numbers, addresses and other personal data of 143 million Americans. That's 44 percent of the total U.S. population and 57 percent of U.S. adults 18 years and older. This is far worse than the average data breach. Hackers stole more than credit and debit card numbers ... with all the personal info stolen from Equifax, hackers can steal your *identity*. They can open new accounts, credit cards, loans or commit tax fraud. This is the on-paper equivalent of cloning you just to open new accounts in your name.

First, if you haven't already done so, you can [check directly with Equifax](#) to see if you're a part of the breach. Note that if you *have* been impacted, Equifax will offer you a free year of their own credit monitoring service. If you choose to take them up on this offer, note that after your one-year free trial, you will be billed if you do not call to cancel your subscription.

Whether you're involved or not, you'll also want to **check your credit report** for fraudulent activity. The Fair Credit Reporting Act (FCRA) requires each of the nationwide credit reporting companies — Equifax, Experian and TransUnion — to provide you with a [free copy](#) of your credit report, at your request, once every 12 months. You can request your free report at [AnnualCreditReport.com](#).

If you're concerned about identity theft, but have not yet become a victim, you can also **initiate an initial fraud alert**. A fraud alert is free, and the credit reporting agency must indicate that there is an alert on your report whenever a company makes an inquiry regarding your credit. This creates a potential roadblock for identity thieves. When you set an alert with one reporting agency, it must notify the other two agencies (but make sure to verify). Alerts last for 90 days but can be renewed.

If you see something suspicious on your report, or if you simply want to be cautious, you can go a step further and **freeze your credit**. Once your credit is frozen, no one will be able to open new accounts — no new credit cards, no new loans, no new anything that requires a credit check — not even you. There is typically a fee for this service, and usually ranges from \$5-10. To remove the freeze, you'll need to contact each agency once again and request the freeze be lifted. This, again, will come with a small fee.

Another option is to **purchase a credit monitoring service**. Vendors typically track your credit file on a regular basis and send you an alert whenever there is a change — some will even search the deep web for traces of your information. Products and services range in both price, types of service and insurance coverage. Search online for credit monitoring services to decide if this is a worthy investment for you.

To place a fraud alert, contact:

- [TransUnion](#) — 1-800-680-7289
- [Experian](#) — 1-888-397-3742
- [Equifax](#) — 1-800-525-6285

To freeze your credit, contact:

- [Equifax](#) — 1-800-349-9960
- [Experian](#) — 1-888-397-3742
- [TransUnion](#) — 1-888-909-8872

[Frequently Asked Questions \(FAQs\) about the Equifax data breach](#)