


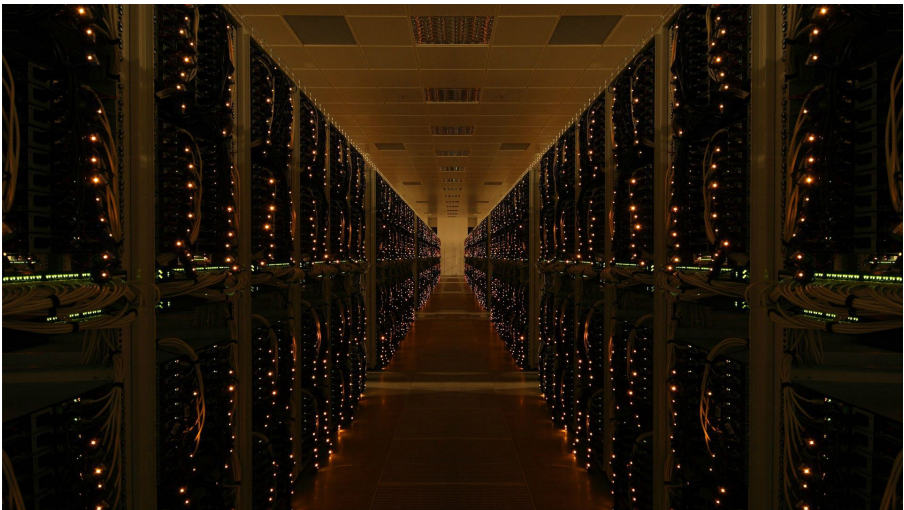


 medium.freecodecamp.org

The Equifax hack and how to protect your family—all explained in 5 minutes

By Quincy Larson | Sep. 15th, 2017

 Send to Kindle



In 1989, the US government decided to concentrate our most sensitive data in the hands of three giant finance corporations: Experian, TransUnion, and Equifax. These three corporations now store our biographic information, every address we've ever lived at, and every major financial transaction we've ever made—all so they can assign us a FICO credit score.

And one of these companies just got hacked.

On September 8, Equifax announced what is now **the worst data breach in history**. And yes—you are most likely a victim of it.

Here's how this whole disaster unfolded.



Get Answers. Take Action.

\ Home

System Currently Unavailable - Error 500

We're sorry. We cannot process your security freeze request online at this time. Please try back later.

To make a security freeze request with the other national consumer credit reporting agencies, please contact Experian, P.O. Box 9554, Allen, TX 75013 (888)379-3742
TransUnion, P.O. Box 6790, Fullerton, CA 92834 (888)909-8872

Thank you for giving Equifax the opportunity to assist you.

Equifax Information Services, LLC

A 500 server error from Equifax when attempting to freeze my credit, along with millions of other Americans.

On March 7, the developers of [Apache Struts](#)—a Java web development framework popular with big finance companies—released a critical security patch.

For more than two months, Equifax failed to apply that patch.

Then in May, attackers discovered that Equifax was vulnerable. They started siphoning data out of Equifax's massive databases.

For more than two months, attackers had full access to the records of 143 million Americans, 44 million Brits, and an unknown number of Canadians.

These records included:

- First and last names
- Social Security numbers
- Birth dates
- Current and past addresses
- Drivers License numbers

In short: everything a thief would need to impersonate you, take all your money, and wreck your credit. For nearly **200 million people**.

Equifax discovered the breach on July 29, and finally applied the patch. They then waited another 38 days to tell anyone about the breach.

During this time, Equifax executives sold \$2 million in stock, in a brazen act of insider trading.

And Equifax has done plenty of other sketchy things:

- Equifax offered consumers a year of free identity theft protection, then tucked a “you waive your right to sue us” clause into the fine print. (They’ve since removed this due to public pressure.)
- Equifax built a “did I get hacked?” website and told people to go there to check whether their data had been breached. But people quickly discovered that the website was answering randomly.
- Equifax started automatically assigning “security PINs” that were just a timestamp from when you froze your credit.

Several government officials have announced criminal investigations into the Equifax breach. And one law firm is launching a \$70 billion class action lawsuit—the largest class action lawsuit in history.

I hate to be the bearer of bad news, but here’s what all this means for you and me: we’re going to spend several hours filling out ugly webforms.

“But how do I know I’m affected?” I hear you ask. There’s no way to know for sure. As we’ve established, Equifax is totally incompetent, and has no clue who has been affected.

But there’s one thing everyone agrees on: [you should freeze your credit immediately.](#)

Unfortunately, you’ll have to push your way past the millions of other Americans who are also frantically trying to freeze their own credit before a thief can destroy it.

The consequences of identity theft are substantial. People struggle for years of their lives trying to fix their credit. But much of this risk is preventable.

You'll need to get credit reports from all three credit rating agencies and store these PDFs somewhere safe in case of a dispute.

This process should be free if you haven't requested one in the past year. And the rating agencies have an official tool for getting all three of these through a single series of web forms: <http://www.annualcreditreport.com/>

Next, you need to freeze your credit with all three credit rating agencies. Then you can unfreeze it later when you need it—hopefully after the current chaos subsides.

Once your credit is frozen, you'll still be able to use your credit cards and pay for any existing loans you may have (cars, mortgages, etc.) But you won't be able to take out any new debt or apply for any new lines of credit (like credit cards.)

This may seem like an extreme measure. But again, it's not just me recommending this. Everyone is recommending you do this.

Oh, and this process will cost you \$10 for TransUnion and \$10 for Experian. (After considerable public pressure, Equifax dropped the fee for freezing your credit—at least until October.)

Here are the links. Be sure to record the PIN they give you at the end of each process:

Equifax: https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp

Transunion: <https://freeze.transunion.com/sf/securityFreeze/landingPage.jsp>

Experian: <https://www.experian.com/freeze/center.html#content-01>

Note that I had one hell of a time trying to freeze my credit. Some of these forms gave me cryptic errors and I had to come back and try again hours later. Stick with it! And remember to do go through this same process again for every adult member of your household.

Birth certificates are the ultimate identifier of you as a human being. They have even more weight than drivers licenses and passports.

Get a copy of a birth certificate for each member of your family. Then put these in a safe deposit box at a bank or a [fire-retardant box](#) hidden in your house.

One of the most common identity theft scams is when a thief files taxes on your behalf, then claims your income tax refund. And thanks to Equifax, all the data that thieves need to do this is now out in the open. So next year, file your taxes as promptly as possible.

Assume that your social security number and other identifying information—like previous addresses and places of work—are now public information.

Keep this in mind when getting calls or emails from banks or governments. Just because the person contacting you knows these facts about you does not mean they are who they say they are. They may be trying to [spear phish](#) you by using the information they have to extract even more information from you.

Thanks to Equifax, these are now precautions that everyone needs to take. If you lock your doors at night, you should lock your identity, too.

What's different now is that identity theft is going mainstream. It may no longer just be stories you hear about a friend of a friend. It may start happening all around you.

Maybe the US government will come up with a better identification system than your social security number—a 9-digit code that you carry with you through your entire life and can't easily change. Maybe it will be multi-factor identification, incorporating some combination of biometrics and secret codes that change from time.

Whatever happens, don't let your guard down. Stay safe out there!

And if you want to read more about how we can prevent these types of breaches in the future, read security expert Bruce Schneier's op-ed on [how we should regulate data brokers like Equifax](#).

Thanks for writing this, Quincy. I clapped 50 times even though that took me longer than it took to freeze my credit.

It's not just your credit that's in jeopardy. With that information, a fraudster can open investment accounts, bank accounts and take out insurance policies. Check out the *Patriot Act, Title III, Sec. 326. Verification of identification* for all the legalese. Why would opening new accounts matter you say? Better call Saul to explain Money Laundering.

Quincy, you deserve a medal for this. A super secure titanium one with facial recognition.



Thanks for the detailed but brief guide. There needs to be some repercussions for Equifax. Pretty much **everyone** is affected by Equifax's negligence. What they did, and how they're handling it, is absolutely horrendous, and I can't think of a suitable

punishment for them. Any sort of fee or jailtime just seems like a slap on the wrist, compared to the hundreds of millions of lives it has affected.

Great advice

Quincy Larson

Going through this miserable and preventable process will hopefully get our government and behemoth companies bestowed these legal monopolies serious about cyber security and the modern era.

Great article. Unfortunately, Equifax servers haven't been up to the challenge for days, Transunion is unable to confirm my account, and Experian denies my online request and wants me to snail mail a ton of information. Ugh. Here we go....

Even though I live in Norway and this doesn't affect me, it was really interesting information to process.

We have 3 major credit report companies in Norway as well. One of them is Experian. In order to protect myself for future identity theft, I froze all my information at those 3 companies 6 months ago. 2 of them I closed...

Thank you Quincy Larson for this helpful piece.

I just walked a co-worker through this and she was able to freeze her Experian and Transunion files online quickly and pretty easily. Equifax didn't work initially but she had to guess one of the ID verification questions, may have gotten it wrong. She's going to try again when...

Annual credit report.com seems to have a lot of bad reports online about it.

It is the service recommended by the credit agencies themselves. Even though it's UX is pretty meh, it does speed up the process.

Thank you for this! Took me about 30 minutes total for all three. Equifax website "disconnected" me a couple of times but keep trying. They are free, but TransUnion and Experian were \$10 each. Thanks again for making this helpful post.

