October 2017

Frequently Asked Questions (FAQs) about the Equifax data breach

Source: Michigan Credit Union League

Who/What is Equifax?

Along with TransUnion and Experian, Equifax is one of the three major credit reporting agencies in the U.S. They track your entire financial history — every bill you pay, any loans you have, credit cards, credit inquiries and more. They use this information to generate your credit report. When you apply for a new loan, credit card or attempt to open any new account, businesses look at your individual report to decide whether or not they want to lend you money, how much money to lend and at what interest rate.

What happened?

According to Equifax, hackers breached their system from mid-May through July. They got names, Social Security numbers, addresses (current and past), birthdates and, in some cases, driver's license numbers 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. Equifax waited six weeks to announce the breach.

What does it mean for me?

Recent hacks and data breaches with major retailers like Target, Home Depot, Wendy's and others have put the public, credit unions and banks in a tough position. Under current law, retailers are not required to pay the costs to send individuals their new debit/credit cards, and generally pay none of the fraudulent charges hackers rack up. Who is stuck paying these costs for data breaches? Your credit union or bank — and ultimately, you.

If that sounds bad, this is even worse. When hackers steal a credit or debit card, they have access to an isolated account. They can do damage, but it's isolated damage. With all the personal info stolen from Equifax, hackers can steal your identity. They can open new accounts, credit cards, open loans and commit tax fraud. You won't even know about it until you're in massive debt and it has damaged your credit.

What can I do?

You have several options. Most are free, but take time. Several extra measures come with a price tag. You'll want to look at the pros and cons of each.

Check the Equifax registry

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. Be wary and read carefully before clicking.

Check your credit report

MCUL
MICHIGAN CREDIT UNION LEAGUE & AFFILIATES

If Equifax reports that you are, in fact, involved in the breach, you'll 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. Rather than requesting all three at once, consider staggering them out every four months so that you can check your status throughout the year.

Place a fraud alert on your reports
If you're concerned about identity theft but have not yet become a victim, you can 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.

Note that: 1) the alert lasts for 90 days but can be renewed, and 2) when one credit reporting agency places a fraud alert on your file, it must notify the other two agencies. To place an initial fraud alert on your file, contact one of the three credit reporting agencies:

- TransUnion — 1-800-680-7289
- Experian — 1-888-397-3742
- Equifax — 1-800-525-6285

Freeze your credit
If you see something suspicious on your report, or if you simply want to be cautious, you can put a freeze on your credit. According to the Federal Trade Commission (FTC), "this tool lets you restrict access to your credit report, which in turn makes it more difficult for identity thieves to open new accounts in your name." There is typically a fee for this service and usually ranges from $5-10.

To freeze your credit, you'll need to contact each of the three credit reporting agencies:

- Equifax — 1-800-349-9960
- Experian — 1-888-397-3742
- TransUnion — 1-888-909-8872

Note that once your credit is frozen, even *you* will not be able to open new accounts — no new credit cards, no new loans, no new anything that requires a credit check. 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.

Enroll in a credit monitoring service
There are many credit monitoring services on the market that do exactly that — monitor your credit. They typically track your credit file on a regular basis and send you an alert whenever there is a change. 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.

Pay close attention to your accounts

Some people check their savings, checking, loan and credit card accounts on a regular basis, others, a bit more casually. If you're the latter, you'll want to start paying closer attention. You know your own spending habits best and should be able to notice if something goes wrong with one of your currently-open accounts.

Contact state and federal lawmakers
Five years ago, hardly anyone talked about data breach. Now it seems like a monthly occurrence. As mentioned earlier, a large part of the problem is that this is a *new* problem, and the law hasn't evolved to keep up with the situation.

Again, when retailers are hacked and your information is stolen, they're not required to pay the costs to send you a new debit or credit card and generally pay none of the fraudulent charges that might rack up. Under current law, that's covered by your credit union, bank or you. So if merchants can shift the cost of their data breach onto someone else, what incentive is there to increase their data security?

The answer is simple, none.

That needs to change. Your credit union is already battling this in the State Capitol and in Washington, D.C., but can use your help. Visit StopTheDataBreaches.com to learn more and take action.

MCUL
MICHIGAN CREDIT UNION LEAGUE & AFFILIATES