

EQUIFAX DATA BREACH – BIG SCAM NEWS

On September 7, Equifax announced it discovered a massive security breach to its consumer credit files. Equifax reported the breach “potentially impacts the personal information of 143 million people, including 1.1 million from Iowa. Hackers gained access to the full name, address, birthdates, social security numbers, and in some cases driver’s license numbers and credit card numbers. Equifax reported it discovered the breach on July 29, 2017, and learned the hackers were in their system from May 13, 2017 until July 29, 2017.

What’s the big deal, or is a big deal? Yup, it’s a big deal. Although it is not nearly the biggest breach of recent times (that dubious records still belongs to Yahoo), it is likely the one with the greatest potential to harm consumers. To understand why, let’s answer a few questions.

What is Equifax? Equifax is a consumer credit reporting agency, headquartered in Atlanta, Georgia. The company collects and compiles information on 800 million people and 88 million businesses around the world. Equifax sells the information it collects to banks, retailers, utilities, governments, healthcare providers, insurance companies, loan companies. That information allows those firms to decide how credit-worthy we are. Equifax is one of the “Big Three” credit reporting agencies (the other two – Experian and Transunion).

Equifax is not a bank, credit union, or a credit card company. Something to remember about Equifax in this deal, is none of us made any agreement with Equifax to share any information with them. They gain information on us from a variety of public and private sources, and we control none of it. This is a difference between Equifax, and, say, Target, which also suffered a big data breach. Anyone with a Target credit card made a conscious decision to share their information with Target, in exchange for credit approval.

What Can Happen With The Information From Equifax? Potentially, a great deal. Breaking into Equifax was like tunneling into Fort Knox and getting the gold bars. In many previous data breaches, the credit card numbers, names, and addresses of consumers got compromised. With Equifax, enough of our personal information was compromised, it would allow all kinds of identity theft to take place on a scale never before seen. And it can happen years from now. You can cancel your credit card numbers or bank account number if those accounts are compromised, but you can’t really change your name and birth date, or change your employment history or address history. Whoever was responsible for this breach, they can hold onto this information for years before acting on it, or selling it to others.

How Do I Know If This Breach Affected My File? Equifax set up a website, <http://www.equifaxsecurity2017.com>, to explain this breach, offer updates, and allow consumers to check their file. One part of the website asks consumers for their last name and

last six numbers of their social security number. That's enough information for Equifax to determine if your file was accessed. Don't use a computer? You can call Equifax at 866-447-7559. Warning – I am reading and hearing from people who report no one answers this number. Evidently the lines are jammed. If you go online, and find out your file was compromised, Equifax offers you an immediate chance to sign up for free credit monitoring. More on that later.

What Should I Do? I've read through the recommendations from the major consumer protection agencies on how to handle this deal. These listed here are measures most of these agencies recommend:

- Order and review your credit reports. You can get your credit report for free once a year from each major credit reporting agency. A lot of folks stagger their request so they view these reports once each four months. Not a bad plan. Go online to www.annualcreditreport.com for the free report. By going online, you'll get the report within minutes. Or you can call 877-322-8228. If you call, expect to wait three weeks for the report to reach you in the mail. When you get it, look for activity on the report you did not authorize.
- Consider a security freeze. A freeze locks out anyone from inquiring about your file, with a few exceptions, like the IRS for example. If you live in Iowa, the charge for a freeze is \$10. It is free from Equifax until November 21. You must ask for a freeze from each of the three credit reporting agencies. You can stop a freeze at any time, but know ahead of time, it can take a few days to lift. A freeze is free if you've been the victim of identity theft.
- Set up a fraud alert. These alerts are free, and you only need to make one call to a credit reporting agency, then that agency will share with the other two. Initial alerts are for ninety days, but can be extended under some circumstances for up to seven years. The alerts don't prevent businesses from viewing your credit file, but they do require anyone planning on extending credit to verify your identity before going ahead.
- Closely read your bank and credit card statements. We should all be doing this already, but now we need to be extra vigilant. You are looking for charges you did not authorize. Check out even small charges. These can be attempts by scammers to see if you are paying attention. If you miss these, scammers will send through larger charges next month.
- Check your mail closely. You are looking for bills on accounts you don't recognize, or notifications of new credit cards issued to you. Also look for mail from Social Security about changes in direct deposit, or the postal service about change of address. Both are warnings of fraud.

- File your taxes as soon as possible. Tax fraud identity theft was rated as one of the most prevalent forms of identity theft last year. You need to get your refund before the scammers do. We just learned on September 19, a payroll subsidiary of Equifax got hacked in March 2017, compromising a lot of W-2 wage statements. From this, I deduce these hackers know how to commit tax identity theft.
- Be wary of other breach-related scams. We can expect to hear of calls or emails from crooks posing as Equifax, wanting to “confirm” this or that. Don’t fall for it.

The question will come up from some readers, “Should I sign up for an ID protection service?” As part of its response to this breach, Equifax is offering one year of free monitoring of your ID, through one of its subsidiaries, Trusted ID Premier. If you go online to the Equifaxsecurity2017 website, you can be directed to this monitoring service to opt in. The US Consumer Financial Protection Bureau (CFPB) warns, however, before signing up, check for:

- Trial periods
- Fees
- Cancellation requirements
- Automatic renewals

CFPB also recommends against providing a credit card or bank account information when signing up, since this will prevent you getting billed at a later date for something unexpected.

This is a dynamic, developing story, and we can expect to hear a lot more about this. Equifax did a lousy job securing this information, and their response to date leaves many questions unanswered. I look forward to what class-action lawsuits, congressional investigations, and investigations by other regulators uncover. Stay tuned.

CONTACT SENIORS VS. CRIME

Let me know about scams, fraud, or other crookedness you run across. Most of what I learn, I learn from you. Contact me at Seniors vs. Crime, Clinton County Sheriff’s Office, 563-242-9211 extension 4433, or email me at randymeier@gapa911.us