FORTALICE CLIENT ADVISORY

EQUIFAX BREACH: Protecting Yourself and Your Business

August 8, 2017

Fortalice

Fortalice

Executive Summary

WHAT HAPPENED AT EQUIFAX?

By now, you have likely heard about the cyber incident announced by Equifax yesterday, September 7th, 2017. You can read the full release from Equifax here (https://www.equifaxsecurity2017.com). This advisory summarizes our thoughts on this incident.

- 143 million Equifax customers have likely been affected by this breach.
- This breach includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers.
- Equifax is working with state, local and federal regulatory industries to assess the damage and find justice.

HIGHLIGHTS

EQUIFAX DATA BREACH

FIRST, this was a breach that provided an outside party with access to a significant data set held by Equifax. In the public press release, Equifax states that this was an incident "potentially impacting approximately 143 million U.S. consumers." If that sounds like an incredibly large number, it is. Considering that in 2016 the United States had a population of approximately 323 million people this estimation means that three out of every four adults in the US are potentially impacted by this breach.

SECOND, the data breach contains sensitive information. According to the release, the data to which the attackers gained access "includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers." Probably less interesting to most readers, but something significant is this line in their notification, "Equifax also is in the process of contacting U.S. state and federal regulators and has sent written notifications to all U.S. state attorneys general, which includes Equifax contact information for regulatory inquiries." This sounds like boring, legal jargon, but the United States is a country that does not have a national data breach law. This means that 48 states – that is every state except for South Dakota and Alabama – each has their own law and requirements for a company when a data breach affects residents of that state. Think about the scale and complexity of the effort faced by Equifax working with every individual state to follow the letter of the law in each and every location. In addition, many of these states have provisions that allow residents to sue companies when such an event occurs. Let me be clear, we are only seeing the tip of the iceberg on this incident and it is going to be a significant event for the future of cyber security in the United States.

THIRD, to date there has been very little data released about the details of the breach, this is to be expected. According to the press release, the breach occurred in Mid-May and was discovered on July 29th. Most readers will probably be surprised that notification of the general public occurred today, over 30 days later, but they shouldn't be. Following the discovery of the breach, an outside firm was likely brought in to perform forensics. This process was not a short one and likely took a minimum of a week or two. Once a breach is confirmed, many states require a notification within 30 days. This indicates that this breach was likely confirmed internally on or around August 8th, 10 days after it was discovered. The data accessed, according to the press release,

was "certain files," while CEO of Equifax states in his video message it was "data files." These files were accessed through a method broadly defined as "a U.S. website application vulnerability."

In addition they are claiming that they "found no evidence of unauthorized activity on Equifax's core consumer or commercial credit reporting databases." This final statement likely means one of two things. Either (A) the attackers were able to exploit something such as a SQL Injection to pull data from servers and didn't gain access to the systems themselves or (B) Equifax may not have been storing the data necessary to "find" evidence of such activities and therefore can make this claim.

FINALLY, it is important to note the actions being taken by Equifax following a breach. Equifax is smart to be following industry best practices for what to do following a breach, as such they have begun the following:

- Engaged a firm to perform a forensics review
- Established a website to provide monitoring services to their customers
- Established a call center to support concerned customers
- Sent written notifications to all affected
- Working with law enforcement
- Notified U.S. state and federal regulators
- Notified all U.S. state attorneys general

It is clear that the scope and scale of the actions required by Equifax following this incident are staggering and the costs associated with this response are going to be enormous. For perspective, the Home Depot breach in 2014 likely cost the company around $179M and that breach only affected 50 million credit card numbers and around 53 million email addresses.[1]

[1] https://www.webtitan.com/blog/cost-retail-data-breach-179-million-home-depot/

REALITY CHECK

SO THE REAL QUESTION IS WHAT DOES THIS BREACH MEAN TO YOU?

FIRST, it is more likely than not that your personal information was included in this breach. If attackers use this information, they could attempt identity theft or other scams. You should make sure that you are monitoring your credit files at the credit bureaus and monitor your credit cards and bank accounts for suspicious activities. Fortunately, Equifax will provide this for free for a year to all affected - it's the least they can do.

SECOND, it is very highly likely that other scammers will exploit this event to try to capture your information. Never give your personal information to anyone over the phone or to a website that you have not verified as being legitimate. If you are told to visit a website in response to a breach (such as Equifax's own website for this incident: www.equifaxsecurity2017.com) never click on a link in an e-mail to that website. It is better to cut and paste the domain name or manually type the domain name in the browser.

We have already seen indications that spammers have shown interest in this event. For example, the domain name released by Equifax was registered on the 22nd of August, however many variants of that domain name were registered today by a different service, likely on behalf of Equifax. This delay is likely the result of some form of an oversight by the company in not considering the fact that a good attacker could use the domain name "equifaxsecuvity2017.com" to trick unwitting customers; notice the "v" instead of the "r" in security. Our assumption was that Equifax's mass registration of these variants was in response to an individual registering the name "equifoxsecurity2017.com." Interestingly enough, visiting that url brings up a website that tells the user "You're probably looking for https://www.equifaxsecurity2017.com/" and then asks the question "Why was I able to register this after the Equifax breach announcement??"

FINALLY, you should certainly be considering if your own infrastructure is exposed to an attack and if you have adequate protections in place. Of course, being a Fortalice client is a great start!

You should also consider if you are prepared to respond in the event a data breach occurs within your company or organization. A good way to evaluate your preparedness is to get into a room with your leadership team and to walk through what would happen if you discovered a data breach. Here are some key questions to consider:

1. Who would be responsible for managing the incident?
2. Who would support the forensics and analysis?
3. What data are you collecting that could help determine the breadth of the attack?
4. Is your law firm prepared to support you?
5. Do you know who to contact in law enforcement?

CONTACT FORTALICE

We are here to help you protect your business. If you are worried your team will not have time to do some or many of these important steps, give us a call. Fortalice is highly skilled in disaster recovery, incident response exercises and cyber risk assessment and we are standing by to aid you and your team in assessing the fallout from this breach.

If you have any questions about implementing these steps, please call us for a no-cost consultative discussion. Fortalice is currently assisting clients with their strategies and is ready assist you.

Contact: Mike Holland
Executive Vice President of Business Development
mholland@fortalicesolutions.com
877.487.8160