Williams Overman Pierce, LLP
Certified Public Accountants and Consultants

Breaking Down the Equifax Data Breach

Equifax, one of the "Big Three" credit reporting agencies, disclosed a massive data breach in a press release on Sept. 7—six weeks after the breach was discovered. Over the course of three months, hackers exploited a website application vulnerability to access the personal data of as many as 143 million Americans—nearly half the U.S. population. The exposed data include names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. Approximately 209,000 credit card numbers and dispute documents with personally identifiable information (PII) for approximately 182,000 consumers were also stolen.

If you weren't personally affected, chances are you know someone who was.

What Went Wrong?[1]

Like Wannacry and Petya before it, the attack on Equifax succeeded because of a failure to install a months-old patch. According to the company's official release, the data breach directly resulted from a delayed implementation of a software security patch to a known web server vulnerability, Apache Struts CVE-2017-5638, first disclosed in March 2017. Apache Struts is a free, open-source framework for creating Java web applications. The CVE-2017-5638 vulnerability mishandles file uploads, enabling an unauthenticated remote attacker to execute arbitrary commands with the privileges of the user running Apache Struts.

Effective patch management remains a struggle for many organizations' IT departments. But what exacerbated the magnitude of the Equifax breach—the second largest on record, after Yahoo—was the company's information governance practices. It created a repository of sensitive information that was far too large. Once the hackers were in, they had access to it all.

Their response also met with public criticism for several reasons: 1) The official website to help consumers determine whether their information was compromised was hosted on an offsite domain, equifaxsecurity2017.com, instead of the secure company website, making it easy for bad actors to misdirect consumers to malicious copycat versions. And in fact, Equifax itself mistook a fake site for the real one, tweeting out links to the fake site multiple times via its official Twitter handle. 2) The equifaxsecurity2017 website redirected visitors to another outside URL, trustedpremierID.com, which flagged to some browsers as a phishing site. 3) Enrolling in the free credit monitoring service offered by Equifax as recompense to victims initially came with strings—an arbitration clause that enraged consumers.

Then there were the three Equifax executives who sold close to $2 million worth of company stock two days after the breach was discovered. Equifax released a statement that said the three executives "had no knowledge that an intrusion had occurred at the time they sold their shares." If true, this means it took more than 48 hours to communicate the incident to senior management.

What's the Potential Fallout?

For Equifax, the road to recovery is a long one. The company has already taken a major reputational hit, its shares dropping 20 percent, worth $4 billion, in the week following the breach disclosure. The damage may not be lasting, however; historically, companies hit by scandal see their stock rebound in a relatively short period of time.

The Federal Trade Commission (FTC) also announced last Thursday that it is commencing a probe of the Equifax data breach. The Consumer Financial Protection Bureau,

[1] Facts related to the nature of the Equifax breach are derived from information Equifax has reported in press releases and public statements.

too, is considering pursuing an investigation of Equifax under a provision of the Dodd-Frank Act banning unfair, deceptive and abusive acts and practices (UDAAP). Regulatory action may revive efforts in Congress to pass data privacy legislation and increase oversight of credit bureaus.

For the victims of the breach, what the hackers plan to do with the stolen PII remains to be seen, as their motive and identity is unknown. One likely outcome is the sale of private information exposed by the breach on the dark web. This PII can be used by criminals to commit identity theft, perpetrate bank-related fraud or even to augment stolen healthcare records with incomplete PII for fraudulent billing purposes.

What do I do now?

Individuals should:

- **Request a one-time credit freeze** from all three major credit bureaus. Equifax has stated it will waive credit freeze fees through November 21. You shouldn't have to pay more than $5-$10 to freeze your credit files through TransUnion and Experian. Watch out for more expensive options with monthly fees for additional services you may not need, and keep in mind that a freeze prevents you from getting new credit.
- **Sign up for ongoing credit monitoring** from both your respective credit card companies as well as an independent credit monitoring firm. The free credit monitoring service from Equifax is only good for one year. Your Social Security number is forever.
- **Be on the lookout out for suspicious emails and phone calls.** The FTC has already posted an alert warning consumers of a potential related phone scam.

Businesses should:

- **Implement a risk-based, threat-driven patch management program.** Organizations must be able to identify system vulnerabilities and relevant patches in a timely manner, understand the degree of risk the vulnerability presents, and work with asset owners to deploy the update. We suggest 72 hours or less after software patch release to reduce vulnerability to such cyber attacks.
- **Monitor 24/7/365.** To be cyber resilient, organizations need to have threat monitoring and analytics tools to detect an attack, as well as the investigative and digital forensics capabilities to understand what went wrong and the scope of the damage.
- **Develop and test an incident response plan.** Learn from Equifax's mistakes and make sure you have an up-to-date response plan in place to mitigate the impact of a cyberattack, notify critical stakeholders and quickly restore trust.
- **Perform an independent cyber risk assessment annually and penetration testing at least quarterly.** A cyber risk assessment and regular penetration testing can help organizations stay on top of cyber vulnerabilities and emerging threats and close any security gaps.
- **Establish a positive working relationship with your local FBI office** before a breach occurs so you know who to call and what to do when it does. The FBI is there to help; its role is not to find fault or lay regulatory blame on a victim organization, but rather to conduct the investigation in cooperation with the victim organization and determine who perpetrated the attack.