Equifax: What Companies Should Learn From The Largest Data Breach in U.S. History

Matthew J. Schiller, Peter B. Phillips, Mitchel S. Kay

Greenbaum, Rowe, Smith & Davis LLP Client Alert
September 21, 2017

The Equifax breach of consumer data, as has been widely reported in the media, may have exposed the sensitive personal information of as many as 143 million people in the United States, along with the credit card accounts and related documents of many customers. The breach exemplifies the potential scope and damage a cyberattack may have on both companies and individuals.

Every company should use the Equifax breach as a learning experience in order to sufficiently plan to protect itself from cyberattacks. The current adage concerning cybersecurity breaches is that there are three types of companies: (1) those that *have* been hacked, (2) those that *don't know* they have been hacked, and (3) those that *will* be hacked.

A company's data can be breached intentionally (e.g. disgruntled employee, nation-states, hacktivists) or unintentionally (due to inadvertent disclosure by an employee or independent contractor). Every company should be aware of the following:

- **Communication is Key.** In the event of a data breach, a company must determine how to communicate the news to the public and its customers. Companies should create a customized notification plan and related protocols in the event of a potential data breach. Although state and federal statutes only provide minimum disclosure requirements at this time, a company may choose to take actions extending beyond the minimum requirements in order to maintain customer goodwill and potentially mitigate any damages incurred as a result of the breach.

- **Every Company is Vulnerable.** All companies are susceptible to data breaches, regardless of their best efforts and protections. A company is only as strong as its weakest link or most vulnerable point of entry. Companies should prioritize the protection of all systems, servers and programs, and should engage an outside consultant (in the absence of in-house capabilities) to explore potential vulnerabilities in a testing environment. Employees should be trained to spot a phishing attempt and take appropriate action. "Insider" behavior should be closely monitored, and an exit strategy for the voluntary or involuntary departure of employees should be implemented.
- **Review IT Agreements.** It is vital that companies carefully audit, review, and if necessary re-negotiate and revise all IT and third-party outsourcing agreements (e.g. software, cloud-related, hardware, consulting). These agreements should clearly delineate liability and responsibility in the event of a data breach and set forward steps in the event of such an incident.

- **Protect Company Assets Through Cyber Liability Insurance.** All companies should take time to review their insurance policies to ensure that such policies have adequate coverage to protect against a potential data breach and cybercrime.

Issues related to cybersecurity bring innumerable complex issues into play, and there is no one-size-fits-all solution. Planning should involve a coordinated effort by the company’s IT advisors, a cybersecurity forensic firm and legal counsel to establish the maximum level of cybersecurity protection.

Individuals who believe their personal information may have been compromised due to the Equifax breach are advised to review the official guidance of the Federal Trade Commission (FTC) which can be accessed at: https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do.

If you have any questions regarding the issues outlined in this Alert, please contact the authors, **Matthew J. Schiller, Peter B. Phillips** and **Mitchel S. Kay**.