Subscribe To Data Privacy Law

Email Address *

SUBSCRIBE!

Search Posts

Categories

- Webinars & Podcasts
- Jaffe Updates
- News
- Electronic Payments Law +
- Michigan Green Law +
- Data Privacy Law +
- Immigration Law +

Download PDF

OCTOBER 16, 2017 | JON SRIRO

Consequences of and Lessons Learned from the Equifax Data Breach

The Equifax data breach has and will have significant long-term ramifications for data security practices and personal privacy. Understanding how the Equifax data breach occurred and the type of data compromised is crucial to understanding the consequences of this breach.

Reason for the Data Breach

Based on available information, it appears that the hackers were able to breach Equifax's security due to an application vulnerability that was running on its server. Specifically, there was a vulnerability with Apache Struts 2. Apache Struts 2 is an open-source web application framework for developing Java EE web applications. A patch for the application was available, which would have prevented the breach, but the patch was not installed.

Data Compromised

The data compromised from the Equifax breach includes names, dates of birth, addresses, driver's license information, credit card numbers, and knowledge-based authentication information. Knowledge-based authentication ("KBA") is a means to authenticate the identity of a user by asking one or more questions the end-user has already supplied the answer to during a registration or interview process. For instance, the following are some typical KBA questions:

- What street did you grow up on?
- What is your mother's maiden name?
- What elementary school did you attend?

Use of Encryption

The personally identifiable information ("PII") stored by Equifax was not encrypted.

Ramifications

The estimated number of people affected by the Equifax data breach exceeds 145 million people. The large number of people who's PII was compromised leads to numerous questions, the answers to which will be dependent on the extent that the PII compromised is distributed, the manner in which it is used, and the extent to which it is used. There are several issues, among many others, that may arise if the PII is widely distributed or comprehensively used:

- The usefulness of KBA may be diminished (many already state it is an ineffective authentication tool). The reason for this is that if the knowledge-based information becomes widely distributed or used, its effectiveness as a viable means to confirm the identity of a person will be (further) diminished.
- The pursuit of tort claims may become more difficult for future data breaches. If an individual's PII is no longer secure and if it has already been compromised, issues related to a proximate cause may be clouded or more difficult to establish. If Company X's server is breached and the compromised PII is substantially the same as the data compromised in the Equifax data breach, the issue of whether the damages flowed from the data breach of Company X or from the Equifax data breach may arise.
- However, it is also likely (perhaps more likely) that it could become more difficult for companies to defend claims involving data breaches. Courts may look at data breaches similar to how the Court in Summers v Tice, 33 Cal.2d 80 (1948) analyzed the negligent conduct of two tortfeasors. Continuing with the Company X example, the courts may place

the burden on Company X of establishing that the breach of its network was not the cause of the damages, which could be a daunting burden of proof to satisfy. If the courts require companies defending identity theft based claims to prove that the complained of damages are not related to their data security breach, the pursuit of claims against companies with lax or insufficient security measures could become much easier.

Lessons

There are numerous lessons we can learn from the Equifax data breach, which include, but are not limited to, the following:

- All PII or sensitive data that is transmitted or at rest should be encrypted.
- Audits of software used internally or by vendors that store or access PII or sensitive data should be performed periodically in order to determine: a,) the type of open-source software being used; b) the version of the open-source software being used; and c) whether the latest security patches have been installed.
- Companies should consult with information privacy professional to review and suggest updates to its technical, physical and administrative data security safeguards.
- PII should only be maintained for the limited purpose for which it was collected and then, once that purpose has been satisfied, it should be deleted.
- Consumers should place a security freeze (a/k/a a “credit freeze”) on their credit with the four main credit reporting agencies: Equifax, Experian, TransUnion, and Innovis. Security freezes should also be placed upon the credit of one’s minor children and anyone one is a guardian or conservator over.
- Consumers should create and safeguard their Social Security Account at https://www.ssa.gov/myaccount. It is important to do this before a criminal does so and hijacks your account.
- File your tax return as early as possible to prevent a criminal from filing before you. The IRS will reject a tax return that is filed after the first one is filed.
- Safeguard your information when online by a) using credit cards for purchases versus debit cards; b) clearing your login information from your browser and not saving your login information in your browser, and c) only provide sensitive information when absolutely necessary and only on a trusted website.