CLIENT ALERTS & INSIGHTS

Data Breach Exposing 143 Million Americans' Personal Information Hits Equifax

SEPTEMBER 12, 2017

Authors: Michael D. Stovsky

Equifax, the international credit reporting agency, confirmed that a data breach exposed the personal information of approximately 143 million U.S. consumers. The breach occurred from May through July of this year. Breached data includes names, Social Security numbers, birth dates, addresses, and even driver's license numbers. Equifax confirmed that the credit card numbers of approximately 209,000 U.S. consumers were exposed as well.

This breach comes on the heels of the largest data breach in history, when Yahoo announced that the personal information of at least 500 million people was breached about a year ago. This breach from Equifax is especially concerning due to the sensitive nature of the data that was breached.

Possible Costs Related to a Data Breach

Data breaches cost organizations enormous sums of money, directly and indirectly. Direct costs include to the amount of money spent to mitigate the consequences of the data breach and to assist individuals whose information has been compromised. Indirect costs can include the amount of money lost through the company's damaged reputation. The average cost for each lost or stolen record containing sensitive and confidential information is $141, and the average size of a data breach in the U.S. is more than 24,000 records per breach.

The biggest losses incurred as a result of a data breach include: remediation (cost to resolve the cause of the breach); loss of customers; business disruption (loss of productivity); regulatory fines (FCC, FTC, and other Federal regulatory agencies); legal costs; notification costs (most states, and some federal regulations, require notification to each data subject); and identity theft repair and monitoring.

Recommendations

In the cybersecurity world, it is often said that the risk of a security incident is a "not an if, but when" question. We recommend that each company immediately take steps to assess its collection of sensitive data. Planning and preparation are the keys to weathering the storm. The very first source of information that government enforcement agencies or plaintiffs' attorneys will look to in the event of an incident is the corporate policies and procedures documenting data handling and security. Companies should have an up to date incident response plan and team in place. Furthermore, the use of encryption, proper employee training, business continuity management, and certain data loss prevention technologies could help reduce losses that may be incurred upon a breach. Companies should also educate their employees, and raise the level of importance that they place on data

security and privacy matters to that of an enterprise risk - with active education, input, and involvement of their boards of directors and C-suite executives and risk managers.

For further information, please contact Michael D. Stovsky, Partner, Benesch, Friedlander, Coplan & Aronoff LLP, 200 Public Square, Suite 2300, Cleveland, Ohio 44115, (216) 363-4626, or mstovsky@beneschlaw.com.

---

[1] 2017 Data Breach Study by the Ponemon Institute and IBM