



NJ Attorney General's Office Assesses Civil Penalties As It Steps Up Efforts to Enforce Data Privacy and Cybersecurity Laws

Client Advisories

10.29.2018

New Jersey Attorney General Gurbir S. Grewal continued his department's efforts to take decisive action to protect consumers from cybersecurity and data privacy threats by entering into two recent settlements with companies it alleges were responsible for the improper disclosure of personal and health information of individuals in several states, including New Jersey.

On September 7, 2018, the Attorney General announced a settlement with an Iowa-based company, Lightyear Dealer Technologies, LLC, that developed software that manages customer and employee information for multiple motor vehicle dealerships. In late 2016, a security researcher gained access to Lightyear's computer systems and downloaded social security numbers, dates of birth, driver's license numbers, and banking information for 2,471 New Jersey residents. The settlement followed the Attorney General's investigation into whether Lightyear violated the New Jersey Consumer Fraud Act and/or the New Jersey Identity Theft Prevention Act. Although Lightyear had previously complied with NJ laws requiring it to give notice of the breach to the affected NJ residents and did not admit that it had violated any NJ statutes, it nevertheless agreed to implement specific cybersecurity measures and to pay a minimum settlement assessment of \$60,784.

On October 10, 2018, the Attorney General announced that Aetna, Inc. had agreed to a settlement to resolve claims that arose from two data breaches in 2017, resulting in the disclosure of protected health information of hundreds of New Jersey residents among thousands throughout the US. One breach involved a mailing that may have revealed information about people's HIV/AIDS status, and the other a mailing that potentially revealed the identity of people who were participating in a study of atrial fibrillation (or AFib). Under the terms of the settlement, Aetna agreed to initiate security reforms, including training programs, to better protect the privacy of individuals' protected health information. Aetna will also pay a civil penalty of \$365,211.59 to New Jersey.

These settlements follow the May 2018 establishment of a new civil unit, called the Data Privacy & Cybersecurity Section, within the Attorney General's office, charged with bringing affirmative civil actions

against persons and businesses that violate the laws that protect NJ residents and their data privacy rights.

The scope of the duties that businesses who maintain people's personal information and health information vary depending upon a number of factors, as the law evolves and grows more complicated with each passing year. All businesses would do well to seek advice from attorneys, technical forensic computer professionals and insurance brokers-all of whom should have strong experience in data privacy and cybersecurity matters-to minimize the risks involved, including the risk of finding themselves the target of a government enforcement action.

For more information, or if you have any questions regarding this advisory or cybersecurity matters in general, please contact **Archer's Privacy and Cybersecurity Group** members **Robert T. Egan** at 856-354-3079 or REgan@archerlaw.com or **Daniel J. DeFiglio** at 856-616-2611 or DDefiglio@archerlaw.com.

DISCLAIMER: This client advisory is for general information purposes only. It does not constitute legal advice, and may not be used and relied upon as a substitute for legal advice regarding a specific legal issue or problem. Advice should be obtained from a qualified attorney licensed to practice in the jurisdiction where that advice is sought.

Related People



Daniel DeFiglio

Partner

✉ ddefiglio@archerlaw.com

☎ 856.616.2611



Robert T. Egan

Of Counsel

✉ regan@archerlaw.com

☎ 856.354.3079

Related Services

- Data Privacy & Cybersecurity

Attachments

Client Advisory- NJ Attorney Generals Office Assesses Civil Penalties As It Steps Up Efforts to Enforce Data Privacy and Cybersecurity Laws

