Arnall Golden Gregory LLP
Attorneys at Law

Daily Privacy & Consumer Regulatory Alert

Published by the Privacy and Consumer Regulatory Practice | Washington, DC Office

June 13, 2019

FEDERAL DEVELOPMENTS

NIST Software Security Framework

On June 11th, the National Institute of Standards and Technology (NIST) released the "Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework." The framework is a white paper draft of proposed guidelines for developers and cybersecurity professionals to incorporate data security and privacy into the design of the software. The framework is intended to help reduce the number of vulnerabilities and mitigate the potential impact of those vulnerabilities. In the future, NIST anticipates that the federal government and businesses purchasing software will be able to use the framework to evaluate the cybersecurity of the products. NIST requested public comment on the draft through August 5th.

FTC Data Security Settlement

On June 12th, the Federal Trade Commission (FTC) announced a settlement with LightYear Dealer Technologies, LLC for allegedly failing to implement adequate data security standards, in violation of the FTC Act and the Gramm-Leach-Bliley Act Safeguards Rule. LightYear, which also does business as DealerBuilt, is an Iowa-based company that sells software and data services to automobile dealerships. The FTC alleges that LightYear failed to implement readily available and low-cost measures to protect the personally identifiable information (PII) of customers obtained from automobile dealerships. The lack of data protection measures led to a data breach in October 2016, which exposed the PII of 12.5 million of consumers – including names, addresses, birth dates, and Social Security numbers. LightYear allegedly stored and transmitted PII in clear text, without access controls or authentication protections, and stored backup data on an unencrypted server. Under the settlement, LightYear will implement more specific security requirements and is required to obtain third-party assessments of its information security program every two years.

OTHER DEVELOPMENTS

Mobility Data as PII

On June 10th, the National Association of City Transportation Officials (NACTO) published a policy report entitled, "Managing Mobility Data," which argues that mobility data should be defined as PII and protected accordingly. According to the report, mobility data, or geospatial data, becomes PII when it is combined with other data, such as a phone number, or when recognizable travel patters can be identified, such as a person driving from home to work every day. The report makes recommendations for cities and localities to consider when managing mobility data and individuals' privacy, including:

- Ensure that city data protection practices are routinely updated to address security vulnerabilities;
- Require mobility companies and vendors to meet industry data protection and privacy standards;
- Clearly define in user agreements the purpose for the collection and analysis of data and only collect the data that is necessary to achieve that purpose; and
- Make de-anonymized data portable.

DNS Security

On June 12th, the Global Cyber Alliance published a report on the economic value of Domain Name System (DNS) security. DNS firewalls automatically prevent users from visiting known malicious websites, such as when phishing scams send malicious links in emails. The report analyzed the 11,000 data breaches reported in the Verizon Data Breach Investigations Report. The report found that DNS firewalls could have mitigated one third of the incidents studied and could have prevented $10 billion in losses over the last five years.

Pediatrics Healthcare Provider Data Breach

On June 13th, *HIPAA Journal* reported that a former nurse employed with Takai, Hoober & Hso Pediatrics in Germantown, Maryland was fired for allegedly improperly accessing the protected health information (PHI) of 16,542 patients and selling the PHI to a third party to use in fraudulent activities. The nurse allegedly stole names, dates of birth, Social Security numbers, and addresses of the parents of the pediatric patients.

This newsletter is published by AGG's Privacy and Consumer Regulatory Practice. For more information, please visit www.agg.com or contact Bob Belair, Kevin Coy, or Montserrat Miller. To subscribe, please email dpcra@agg.com.