Arnall Golden Gregory LLP
Attorneys at Law

Daily Privacy & Consumer Regulatory Alert

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

July 9, 2018

FEDERAL DEVELOPMENTS

FTC Enforcement

On July 5th, the FTC announced that a federal court issued a court order against a company for allegedly deceiving consumers with fake rental property advertisements and enrolling them into a costly credit monitoring service. According to the FTC complaint, Credit Bureau Center, LLC placed advertisements on Craigslist for fake rental properties or properties it had no right to offer rent. The defendants impersonated property owners and offered property tours if consumers would first obtain credit reports and scores from their websites, which claimed to provide them for free. However, the websites enrolled consumers into a credit monitoring service with monthly fees. The order found that the defendants violated the FTC Act, the Restore Online Shoppers' Confidence Act, the Fair Credit Reporting Act, and the Free Annual File Disclosures Rule. Under the order, the defendants are:

- Banned from selling any credit monitoring service with a negative option feature and from misrepresenting material facts about any product or service;
- Required to make certain disclosures when offering free credit reports and to first obtain consent before using customers' billing information to receive payment; and
- Required to pay $5.2 million.

INTERNATIONAL DEVELOPMENTS

EU Parliament Passes Non-Binding Resolution Regarding Privacy Shield

On July 5th, the European Parliament passed a non-binding resolution calling on the European Commission to suspend the Privacy Shield agreement, unless the U.S. fully complies by September 1st. Members of Parliament (MEPs) cited the recent Facebook-Cambridge Analytica incident as evidence that Privacy Shield does not ensure adequate protection of citizens' personal data, especially since both companies are certified under the agreement, and called for the removal of companies that have misused personal data from the Privacy Shield list. MEPs also highlighted the recent enactment of the U.S.'s Clarifying Lawful Overseas Use of Data Act, which grants law enforcement access to personal data across borders, saying that the law could have "serious implications" and could conflict with EU data protection laws (previously reported).

EDPB Holds Second Plenary Meeting

The European Data Protection Board (EDPB) recently provided an update following its second plenary meeting earlier this month regarding various data protection issues. Topics discussed during the plenary included:

- Consistency and the cooperation mechanisms, sharing experiences on the functioning of the One-Stop Shop mechanism, and the performance of the Internal Market Information System (IMI), which serves as the IT platform for exchanges on cross-border issues;
- The EU-U.S. Privacy Shield agreement, with concerns relating to the appointment of a permanent U.S. ombudsperson and formal appointments to the U.S. Privacy and Civil Liberties Board; and

- The adoption of a letter to the Internet Corporation for Assigned Names and Numbers (ICANN), providing guidance to enable ICANN to develop a GDPR-compliant model for access to personal data processed in the context of WHOIS database.

OTHER DEVELOPMENTS

NAPBS Releases Report

The National Association of Professional Background Screeners recently released its second annual background screening survey of Human Resources professionals that found a majority of employers conduct background screenings. The top reasons for conducting background screenings were public safety; improving the quality of hires; compliance with regulatory requirements; and protecting company reputation. Other key findings include:

- 95 percent of employers stated their organization is conducting one or more types of employment background screening, a slight decrease from the first report;
- 86 percent of respondents stated they are screening all full-time employees, a slight increase from 83 percent in 2017; and
- 68 percent of respondents are including part-time employees in their screening process, a slight increase from 67 percent in 2017.

Healthcare Data Breaches

According to data posted on the Department of Health and Human Services' website, 165 cyber incidents were reported so far this year affecting approximately 3.2 million individuals. Of the 165 incidents reported, 70 involved unauthorized access/disclosure, 59 involved hacking/IT incidents, 32 involved theft/loss, and 4 involved improper disposal. The top healthcare-related data breaches involved the:

- California Department of Developmental Services, which experienced the theft of 12 computers containing medical records on 582,174 individuals;
- LifeBridge Health, which was the result of a malware attack that exposed the protected health information of 538,127 individuals; and
- Oklahoma State University Center for Health Sciences, which experienced a network server hack that affected 279,865 individuals.

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.