NEWS

No Harm, Yes Foul: FTC Rules Risk of Consumer Harm Sufficient to Find LabMD Liable for Security Breach.

08.02.2016

In a unanimous decision published Friday, July 28, attached **here**, the Federal Trade Commission (FTC) overruled an administrative law judge and found that a medical testing company's lack of security measures violated federal law, a decision that could increase privacy and security enforcement actions against businesses that process and store personal information, especially health care facilities. For the first time, the FTC held that demonstrating actual financial or other harm to individuals whose information is exposed (such as identity theft or the misappropriation of personal health information) is not necessary; rather, it is sufficient that the information was exposed and that the company did not take reasonable security measures to prevent its exposure. Further, the decision signals the FTC's increased enforcement against health care companies whose data breaches ordinarily are handled under HIPAA by the Department of Health and Human Services.

The decision is the latest in the FTC's adjudication action against LabMD for the exposure of personal and medical information of more than 9,000 patients on a public file sharing network in 2008, and the 2012 discovery of information on at least 500 patients in the hands of identity thieves. Commencing in 2013, the FTC issued a complaint against LabMD alleging that its privacy and security failures constitute an unfair and deceptive trade practice in violation of Section 5 of the FTC Act.

A practice is "unfair" within the meaning of the Act if "it causes or is likely to cause substantial consumer injury." In his November 2015 opinion, Judge Chappelle found that FTC counsel had not proven that the exposure or limited exposure of some LabMD documents in 2008 caused, or was likely to cause, substantial consumer injury, or that the data breach in 2012 was even the result of any alleged computer security failure of LabMD. In its Friday opinion, however, the FTC concluded that an injury to consumers need not have manifested in order for the Commission to address it. In addition, it held that both the probability of injury occurring and the magnitude or severity of the potential injury should be considered. Essentially, the FTC's test boils down to a cost-benefit analysis: if the company took reasonable security measures to combat privacy and security breaches, then its business practices are not "unfair" within the meaning of Section 5 of the FTC Act.

So, "what are reasonable security measures?" Some of the precautions that the FTC found LabMD lacked offer a roadmap. Taking into consideration the "sensitivity and volume of consumer information [the company] holds, the size and complexity of its business, and the cost of available tools to improve security," the FTC assesses the following business practices:

1. Developing and maintaining a comprehensive cybersecurity and information management

program,
2. Routinely deleting customer data that do not need to be maintained,
3. Utilizing automated instruction detection systems,
4. Employing file integrity monitoring software and system penetration testing,
5. Monitoring traffic coming across firewalls,
6. Providing employees with data security training,
7. Limiting or monitoring employee's access to sensitive information,
8. Restricting employee's administrative rights and their ability to modify computer settings and download software.

Given businesses' increasing reliance on information technology and the rise in data breaches in recent years, it is advisable for companies to implement cybersecurity programs that encompass the recommendations enumerated above and address any other vulnerabilities unique to their industry. While businesses certainly cannot guarantee impenetrable privacy and security of consumers' information, taking a realistic and holistic approach to data management and preservation is a good first step.

Related People

- Robert Van Arnam – 919.981.4055 – rvanarnam@williamsmullen.com

Related Services

- Intellectual Property
- Data Protection & Cybersecurity
- Health Care