DrinkerBiddle

Client Alert

August 4, 2016

FTC Overturns Administrative Law Judge's LabMD Ruling on Appeal

By Katherine E. Armstrong and Anthony D. Glosson

Key Takeaways:

- The FTC reverses Administrative Law Judge's decision and concludes that LabMD's data security practices constitute an unfair act or practice under Section 5(n) of the Federal Trade Commission Act.
- The Commission held that the privacy harm resulting from the unauthorized disclosure of sensitive health or medical information is in and of itself a substantial injury under Section 5(n) (the FTC's unfairness authority). The case was decided unanimously with no dissenting statements.
- The Commission's decision is likely to be appealed to the Court of Appeals.
- This is the first data security action litigated before the Commission and the first appealable Commission opinion in a data security action.

The Federal Trade Commission (FTC), on July 29, 2016, vacated Chief Administrative Law Judge D. Michael Chappell's Initial Decision dismissing the FTC's data security complaint against medical testing company, LabMD, Inc. ("LabMD"). LabMD was the first litigated data security action before the FTC.

LabMD, based in Georgia, operated as a clinical laboratory from 2001 to 2014. It conducted tests on patient specimen samples and reported the test results to its physician customers. Over the course of its operations, it collected sensitive personal information for over 750,000 patients. In 2005, a P2P file-sharing program was downloaded and installed on a computer used by a LabMD employee, which the employee used primarily for downloading and listening to music. In 2008, a forensic analyst employed by a data security company discovered and downloaded a copy of one of LabMD's insurance aging reports using a P2P network and standard P2P application to download the file from a LabMD IP address. This file is referred to as the "1718 file" and contained sensitive personal information for approximately 9,300 consumers, including their names, dates of birth, Social Security numbers, "CPT" codes designating specific medical tests and procedures for lab tests conducted by LabMD and, in some instances, health insurance company names, addresses, and policy numbers.

In 2013, the FTC issued a complaint against LabMD alleging that LabMD failed to reasonably protect the security of consumers' personal data. The matter was litigated before Administrative Law Judge (ALJ) Chappell. In 2015, after the administrative trial, the ALJ dismissed the complaint and found that FTC complaint counsel had failed to carry its burden of proving that LabMD's alleged failure to employ reasonable data security constitutes an unfair practice. Specifically, the ALJ found that the FTC failed to prove LabMD's security practices either caused or were likely to cause substantial injury. The ALJ reasoned there was no injury because the FTC could not identify any consumers who had been physically or economically harmed in the seven years since LabMD inadvertently exposed patient data on a file sharing network. Under Section 5(n) an act or practice is unfair if it (1) causes or is likely to cause substantial injury to consumers, which is (2) not reasonably avoidable; and (3) not outweighed by countervailing benefits.

In a unanimous opinion written by Chairwoman Edith Ramirez, the Commission disagreed and reversed the ALJ's decision. The Commission concluded that "the disclosure of sensitive health or medical information causes additional harms that are neither economic nor physical in nature but are nonetheless real and substantial and thus cognizable under Section 5(n)." In addition, the Commission criticized the ALJ as "coming perilously close to reading the term 'likely' out of the statute" and found that it is appropriate to judge a practice based on the "likelihood that the practice will cause harm at the time the practice occurred, not on the basis of actual future outcomes." The opinion also found that LabMD did not employ basic risk management techniques or safeguards, such as automated intrusion detection systems, file integrity monitoring software, or penetration testing; failed to monitor traffic coming across its firewalls; and failed to provide its employees with data security training.

The Commission concluded that "the privacy harm resulting from the unauthorized disclosure of sensitive health or medical information is in and of itself a substantial injury under Section 5(n), and that LabMD's disclosure of the 1718 file itself caused substantial injury." The Commission relied on a number of its data security settlements involving sensitive medical information, and federal and state laws, including HIPAA and HITECH, which establish the importance of maintaining the privacy of medical

information. The opinion also relied on federal courts that have acknowledged the importance of protecting the confidentiality of sensitive medical information, as well as tort law that recognizes privacy harms that are neither economic nor physical.

The Commission also agreed with the complaint counsel that a showing of "significant risk" of injury satisfies the "likely to cause" standard. Such an interpretation, the opinion noted, is supported by prior Commission cases that the likelihood that harm will occur must be evaluated together with the severity or magnitude of the harm involved. Accordingly, the Commission found that the ALJ was incorrect in equating "likely to cause" injury with the probability of injury, finding that a practice may be unfair if the magnitude of the potential injury is large, even if the likelihood of the injury occurring is low. Further, the Commission noted that in *Wyndham*, the Third Circuit interpreted Section 5(n) in a similar way when it explained that a defendant can be liable for practices that are likely to cause substantial injury if the harm was "foreseeable."

LabMD has 60 days to file a petition for review with the U.S. Court of Appeals.

While the Commission has been criticized for blindly supporting complaint counsel when administrative matters are appealed to the Commission, Chairwoman Ramirez's opinion is well reasoned and carefully applies existing legal precedent to the facts developed at trial. The Commission's decision is significant but narrow, focusing on the privacy harm resulting from the unauthorized disclosure of *sensitive health or medical information*. There will be a renewed focus on what is sensitive health or medical information. In addition, the applicability of this narrow holding to Big Data, the Internet of Things (IoT), and other types of sensitive personal information will enjoy close scrutiny.

Drinker Biddle continues to follow the developments in this case and will provide updates as events warrant.

Questions or concerns? The Information Privacy, Security and Governance Team at Drinker Biddle can help.

Information Privacy, Security and Governance Team

Primary Contacts

Katherine E. Armstrong
Counsel
Washington
(202) 230-5674
Katherine.Armstrong@dbr.com

Anthony D. Glosson
Associate
Washington
(202) 230-5131
Anthony.Glosson@dbr.com