29 No. 10 Westlaw Journal Software Law 5

Westlaw Journal Software Law
***1**
August 24, 2016

Data Security
By Jason Schossler

FTC FINDS LABMD LIABLE FOR 'UNFAIR' SECURITY PRACTICES
In re LabMD

The Federal Trade Commission has found cancer-testing laboratory LabMD Inc. liable for failing to provide reasonable cybersecurity protections for patient and insurance information.

In re LabMD Inc., No. 9357, 2016 WL 4128215 (F.T.C. July 29, 2016).
In a unanimous ruling, the commission overturned Chief Administrative Law Judge D. Michael Chappell's dismissal of an FTC enforcement action alleging the laboratory violated Section 5 of the FTC Act, 15 U.S.C.A. § 45.

Writing for the commission, Chairwoman Edith Ramirez said LabMD's security practices were unreasonable, "lacking even basic precautions to protect the sensitive consumer information maintained on its computer system."

The commission also said Judge Chappell erred in ruling that the commission's complaint counsel failed to prove LabMD's allegedly unreasonable conduct constituted an unfair trade practice because there was no evidence consumers had been harmed by the exposure of their personal information.

A privacy harm stemming from the unauthorized disclosure of sensitive health or medical information "is in and of itself" a substantial injury under Section 5(n) of the FTC Act, Ramirez said.

In conjunction with the opinion, the commission issued a final order requiring LabMD to establish a comprehensive information security program to ensure that it reasonably protects consumers' personal information.

The order also requires LabMD to obtain periodic independent, third-party assessments regarding the implementation of the information security program and to notify consumers whose information was exposed through the security breaches.

Security breaches

According to its administrative complaint filed in August 2013, the commission alleged that in two separate instances, LabMD exposed the personal information of nearly 10,000 consumers.

The complaint alleged that in 2008, a LabMD spreadsheet containing insurance billing information of about 9,300 consumers was found on LimeWire, a peer-to-peer network usually used to share music or movie files online.

The information included names, dates of birth, Social Security numbers, health insurance data and policy numbers, the complaint said.

The FTC also alleged that in 2012, the Sacramento Police Department in California found LabMD documents in the possession of identify thieves. The documents allegedly contained the names, Social Security numbers and, in some cases, the bank account information of hundreds of consumers.

These purported security breaches occurred because LabMD failed to use readily available measures to prevent and detect unauthorized access to personal information, the complaint said.

'Hypothetical' harm

***2** Dismissing the complaint last November, Judge Chappell said the commission failed to prove LabMD's alleged failure to employ reasonable data security measures constituted an unfair trade practice under the FTC Act.

At best, the commission showed a "possibility" of harm, but not any "probability" or likelihood of harm, Judge Chappell said.

"Fundamental fairness dictates that demonstrating actual or likely substantial consumer injury under Section 5(n) [of the FTC Act] requires proof of more than the hypothetical or theoretical harm that has been submitted by the government in this case," the judge said.

Additionally, LabMD addressed and fixed the alleged security breach in 2008, and there was no significant risk that any customers would likely experience harm in the future, Judge Chappell said.

Cognizable injury

In overruling this decision, the commission said Judge Chappell wrongly reasoned that no injury occurred because the FTC's complaint counsel could not identify any consumers who had been physically or economically harmed by the exposure of their personal information.

"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)," Ramirez wrote for the commission.

The ruling also stressed that when evaluating whether a practice is unfair, it is appropriate to judge the likelihood that the practice will cause harm "at the time the practice occurred, not on the basis of actual future outcomes."

This is particularly true in the context of data security, Ramirez said, because consumers generally have no way of discovering whether their personal information has been included in a data breach.

"Even if they do learn that that their information has been exposed, it is very difficult for identity theft victims to find out which company was the source of the information that was used to harm them absent notification from the company," the ruling said.

LabMD will have 60 days to file a petition for review of the FTC's ruling with a U.S. circuit appeals court, the commission

said in a statement.
Judge: D. Michael Chappell
Company: LabMD Inc.
29 No. 10 WJSWL 5

End of Document