ROPES & GRAY

ALERT

Privacy & Data Security

November 24, 2015

ALJ Dismisses FTC Data Security Claims Against LabMD Due to Lack of Actual or Likely Substantial Consumer Harm

Attorneys
Heather Egan Sussman
Douglas H. Meal
James S. DeGraw
Seth C. Harrington
David McIntosh
Mark P. Szpak
Michelle Visser
Deborah Gersh
Timothy M. McCrystal
Laura G. Hoey
David T. Cohen
Adam Winship

On November 13, a Federal Trade Commission administrative law judge dismissed the FTC data security complaint against medical laboratory LabMD,[1] potentially vindicating LabMD's vigorous two-year struggle to deny the FTC's allegations that the company failed to provide reasonable security, as well as to challenge the FTC's authority to regulate data security in the first place. The ALJ does not address the FTC's jurisdiction over data security because the Commission had already rejected LabMD's jurisdictional arguments in denying a LabMD motion to dismiss.[2] But on the merits, the ALJ decision dismissing the complaint could substantially limit the FTC's authority by requiring the FTC to present a strong showing of actual or likely substantial consumer harm to bring an unfair trade practice claim.

The FTC's claims against LabMD centered around two incidents that allegedly exposed the personal information of about 10,000 consumers. In the first – dating back to 2008 – a file containing the names, dates of birth, apparent social security numbers, codes for medical tests conducted, and insurance information for approximately 9,300 individuals was allegedly accessible over the internet through peer-to-peer (P2P) sharing. In the second, hard copy documents that included the names and apparent social security numbers of approximately 600 consumers were allegedly found by Sacramento police in the possession of identity thieves.

In its administrative complaint, the FTC's legal theory was that LabMD's alleged failure to secure data amounted to an unfair trade practice under Section 5 of the FTC Act and that its purportedly deficient data security practices are "likely" to cause harm to consumers – both through those two incidents and through the risk of potential, unspecified data breaches. These types of claims have become a regular FTC practice – over the past decade, the agency has brought many complaints alleging that a company's data security practices were "unfair." What is highly unusual in the LabMD matter is that LabMD chose to fight the FTC claim rather than settle, as many others have, through entering into a consent decree.

Section 5 of the FTC Act gives the FTC authority to address unfair or deceptive trade practices. Section 5(n), however, limits practices that can be considered "unfair" to instances where, among other things, 1) the practice causes or is likely to cause substantial injury to consumers; (2) the substantial injury is not reasonably avoidable by consumers; and (3) the substantial injury is not outweighed by countervailing benefits to consumers or to competition. The ALJ's dismissal is based solely on the FTC's failure to establish the first prong of Section 5(n) – actual or likely substantial consumer injury.

In LabMD, the FTC argued there "likely" would be harm, pointing to no particular consumer who had actually suffered harm. The ALJ conceded that "likely" harm could form the basis of an "unfairness" claim, but found the FTC's evidence of "likely" harm unpersuasive without evidence of actual harm "even after the passage of many years." Without evidence of actual harm, the FTC had established, at best, the "possibility" of harm, not the "probability" of harm that the ALJ held was required to show substantial consumer harm to be likely for purposes of

[1] *In re LabMD Inc.*, Initial Decision, FTC Dkt. No. 9357 (Nov. 13, 2015).
[2] *In re LabMD Inc.*, Order Den. Resp't LabMD, Inc.'s Mot. to Dismiss, FTC Dkt. No. 9357 (Sept. 14, 2015).

a Section 5 unfairness action: "Fundamental fairness dictates that demonstrating actual or likely substantial consumer injury under Section 5(n) requires proof of more than the hypothetical or theoretical harm that has been submitted by the government in this case."

With respect to the personal information exposed to P2P sharing, the lack of evidence of actual harm through identity theft and the apparent lack of access by anyone intending identity theft led the ALJ to reject the FTC's reliance on survey evidence regarding harm to victims of third-party data breaches. The FTC fared no better with the Sacramento documents that had allegedly been discovered in the possession of identity thieves. Because the documents were found in hard copy, the FTC could not establish that the documents were even obtained from LabMD's computer systems, and thus certainly could not establish that they were obtained due to any alleged data security deficiencies. Importantly, however, the ALJ held that even if unreasonable data security had caused the exposure of the Sacramento documents, the FTC failed to establish that such exposure is likely to cause substantial consumer harm without evidence that the identity thieves used the data. In the ALJ's view, even evidence that personal information fell into the hands of identity thieves may be insufficient to establish likely harm.

Given that the FTC failed to establish likely harm with respect to the two data incidents it could point to, it is unsurprising that the ALJ found the agency failed to establish likely harm with regard to consumers who were not even implicated in either of those incidents. The ALJ observed that it would require "speculation upon speculation" to conclude that LabMD will suffer a future breach "by a presently unknown third-party who, at some undetermined point thereafter, will use the stolen information to harm those consumers." The FTC presented evidence that consumers with personal information on LabMD's system were "at risk" of identity theft, but – as the ALJ pointed out, and the FTC acknowledged – there is no such thing as perfect computer security. According to the ALJ, the FTC may have demonstrated "risk" of identity theft, and perhaps even "elevated risk" due to apparent deficiencies in LabMD's data security. The ALJ held, however, that without establishing the "degree of risk," the FTC could not demonstrate that consumer harm is "probable," and thus "likely" as required by Section 5(n).

Though not the focus of the decision, also of potentially far-reaching consequence is the ALJ's rejection of the FTC's claims based on reputational harm. The FTC had argued that the disclosure of tests for "sensitive conditions" such as sexually transmitted diseases could cause harm "in the form of stigma or embarrassment." After reviewing the legislative history of Section 5(n) as well as prior statements by the FTC, the ALJ held that even if such harm were established as likely – which it was not – subjective feelings "such as embarrassment, upset, or stigma" could not support a Section 5 unfairness claim in the absence of tangible harm. Such a requirement for tangible harm logically should require dismissal, for example, of actions where consumers with exposed payment-card data allegedly faced aggravation or inconvenience of having their cards reissued, but were reimbursed for fraudulent payment-card charges.

LabMD is the first company to stand up to the FTC in an administrative action regarding data security. An FTC defeat may well embolden those facing similar actions to fight rather than enter a consent decree and may well lead the FTC to be more selective in the data security actions they bring.

This decision could also have implications for private data-security litigation, where, to satisfy federal jurisdictional requirements, plaintiffs without established actual injury must prove that injury is imminent. Ironically, the federal government itself – faced with allegations of its own data-security failures in connection with an IRS data breach far more serious than those alleged by the FTC against LabMD – now contends in papers filed just last week that taxpayers whose data was stolen faced no actual or imminent harm.[3]

It is premature, however, to chalk up a LabMD victory or to rely upon it as lasting precedent. The FTC may well appeal to the full Commission, which would consider the matter *de novo*. Even to the extent the LabMD decision

[3] Mem. of Points and Authorities in Supp. of Defs.' Mot. to Dismiss at 1, Wellborn v. Internal Revenue Serv., No. 15-cv-01352 (D.D.C. Nov. 17, 2015) ("[Plaintiffs'] alleged injuries – in general terms, the future threat of a cyber-security breach and the voluntarily incurred costs intended to prevent future theft – are not sufficient to establish an imminent injury that is certainly impending, as required by Article III.").

ultimately may limit FTC authority over data security, the FTC's decision to bring the case also serves as a reminder of the agency's position that it has jurisdiction over data security matters even in cases where, as in the LabMD case, other agencies may have jurisdiction as well.

For more information regarding the Initial Decision in the LabMD matter or to discuss data security practices generally, please feel free to contact Heather Sussman, Doug Meal, Jim DeGraw, Seth Harrington, David McIntosh, Mark Szpak, Michelle Visser, Debbie Gersh, Tim McCrystal, Laura Hoey, David Cohen, or another member of Ropes & Gray's leading privacy & data security team.