ROPES & GRAY ALERT

Practice Group ▪ Practice Group

August 3, 2016

Federal Trade Commission Holds Medical Laboratory Liable for Allegedly Unfair Data Security Practices

On July 29, the Federal Trade Commission ("FTC" or "Commission") issued a unanimous Opinion and Final Order[1] reversing the FTC Administrative Law Judge ("ALJ") Initial Opinion issued November 13, 2015, which had dismissed the FTC's data security complaint against medical laboratory LabMD, Inc. ("LabMD").[2] The Opinion and Final Order, authored by Chairwoman Edith Ramirez, concluded that the ALJ had applied the wrong legal standard in assessing the FTC's claims against LabMD for unfair trade practices or acts related to data security. Specifically, the Commission determined that the ALJ had erred in assessing the injury requirement for unfairness liability codified in Section 5 of the FTC Act.[3] In so ruling, the Commission has attempted to substantially expand its authority over data security cases, both by extending the unfairness doctrine of Section 5 and also by encroaching on subject matter traditionally left to the jurisdiction of other agencies, like the U.S. Department of Health and Human Services ("HHS") Office for Civil Rights ("OCR"). Given LabMD's aggressive litigating position to date, an appeal from this opinion to a federal circuit court is likely. The extent to which the Commission's position is vulnerable to reversal on appeal remains to be seen.

Background and Opinion

The Commission's opinion comes after a long and complicated procedural history between the parties. The FTC's claims allege that two incidents occurring almost eight years ago exposed the personal information of about 10,000 consumers. In the first incident, in 2008, a file containing the names, dates of birth, apparent social security numbers, codes for conducted medical tests, and insurance information for approximately 9,300 individuals was allegedly exposed to public access over a peer-to-peer (P2P) file-sharing service. In the second incident, 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 2013 administrative complaint, the FTC advanced the theory that LabMD's alleged failure to secure this data amounted to an unfair trade practice under Section 5 of the FTC Act. The FTC also alleged that LabMD's purportedly deficient data security practices were "likely" to cause harm to consumers, pointing to these incidents of exposed consumer data and also arguing that LabMD's practices caused a significant risk of future unspecified data breaches.

The FTC's authority to bring enforcement actions against parties engaged in unfair trade practices derives from Section 5 of the FTC Act. Section 5(n),[4] however, limits when a practice may be considered "unfair" to instances where, among other things, (1) a practice causes or is likely to cause substantial injury to consumers; (2) the substantial injury is not reasonably avoidable by consumers themselves; and (3) the substantial injury is not outweighed by countervailing benefits to consumers or to competition, such as cost savings that could be passed on to consumers.

After considering "the whole record relevant to the issues, including the exhibits properly admitted into evidence, deposition transcripts, and the transcripts of testimony at trial," the ALJ issued an Initial Decision dismissing the

[1] *In re LabMD Inc.*, Op. of the Comm'n and Final Order, FTC Dkt. No. 9357 (July 29, 2016) ("Opinion").
[2] *In re LabMD Inc.*, Initial Decision, FTC Dkt. No. 9357 (Nov. 13, 2015) ("Initial Decision").
[3] 15 U.S.C. § 45.
[4] 15 U.S.C. § 45(n) ("Section 5(n)").

FTC's complaint. The Initial Decision states that the FTC had failed to carry its burden to establish the first of the three requirements for unfairness liability set forth in Section 5(n)—i.e., that a practice causes or is likely to cause substantial injury to consumers. As a threshold matter, the ALJ found that "likely to cause" meant "having a high probability of occurring or being true." The ALJ then determined that disclosure of personal medical information could, at most, establish "subjective or emotional harm," which did not by itself rise to the level of "substantial injury" for purposes of the FTC Act. The ALJ also rejected the FTC's argument that the exposure of LabMD information created a likelihood of future injury because no evidence in the record showed that the file exposed by the P2P service had ever been accessed by anyone intending to commit identity theft. Similarly, the ALJ found no evidence in the record that the physical documents had ever been used to harm a consumer.[5]

In its recent opinion, the Commission rejected the ALJ's finding that subjective forms of harm do not give rise to substantial injury. The Commission concluded that the disclosure of sensitive health or medical information could cause concrete harm that, despite being neither economic nor physical in nature, was "nonetheless real and substantial and thus cognizable under Section 5(n)." The Opinion asserted that exposure of medical data could result in embarrassment or reputational harm, and cited recent cases[6] in which the FTC had previously imposed liability for such exposure without alleging that more tangible harm had occurred.

The Commission also rejected the ALJ's finding that for a practice to be "likely to cause" an injury under Section 5(n), the injury must be "probable," holding instead that showing a "significant risk" of injury can satisfy the "likely to cause" standard. The Commission thus found that a practice may be unfair where the "magnitude of the potential injury [resulting from the practice] is large, even if the likelihood of the injury occurring is low." In this case, the Commission concluded that exposed files could have been found on the P2P network, and that the potential harms were significantly large enough to satisfy the "likely to cause" standard.

The Commission also rejected the ALJ's finding that the likelihood of injury was undercut by the absence of evidence showing *actual* harm to consumers between the first incident of data exposure and the date of the ALJ's decision. Instead, the Commission asserted that the ALJ should have "judge[d] the likelihood that the practice will cause harm at the time the practice occurred, not on the basis of actual future outcomes." In support of this interpretation, the Commission noted that its enforcement actions have a prophylactic purpose and that forcing the FTC to wait for harms to become apparent before taking action against unfair practices would undermine that purpose. Here, in the Commission's view, a significant risk of harm was demonstrated by the fact that the file exposed on the P2P network contained "types of sensitive personal information…[that] are very attractive to identity thieves," making it likely that the information would be accessed in a manner that would cause harm to consumers, even if the documents were not actually used to a consumer's detriment.

Having found that a substantial injury either had or was likely to occur, the Commission analyzed the remaining prongs articulated in Section 5(n), which had not previously been assessed by the ALJ. The Commission found that the injuries were not reasonably avoidable because most of LabMD's clients were physicians or other health care providers, and not the actual patients whose medical information could have been exposed. Accordingly, according to the Commission, the patients whose data might be at risk would likely not know that LabMD had handled their data, let alone what security practices LabMD undertook with respect to that data or what steps they could take to

[5] The ALJ also held that there was no evidence to establish any connection between a LabMD computer security practice and the thieves' access of the hard copy documents. The Commission accepted this finding and based its Opinion and finding of liability solely on the documents accessed via P2P.

[6] The Commission cited the following cases: *In re GMR Transcription Services, Inc.*, 2014 WL 4252393, at *4 (Aug. 14, 2014); *In re Eli Lilly & Co.*, 133 F.T.C. 763, 767-68 (2002); Complaint, *In re Practice Fusion, Inc.*, FTC File No. 142-3039 (June 8, 2015).

avoid injury or otherwise protect themselves. The Commission also concluded that there were no countervailing benefits from LabMD's failure to implement security measures to prevent data exposure.[7]

In determining that the practices in question were unfair practices, the Commission also analyzed LabMD's actual practices and concluded that LabMD failed to take even the most basic of precautions, specifically contending that LabMD had no risk-assessment protocol, lacked data-security training for employees, and failed to restrict or monitor employee use of the company's network. The Commission compared these alleged failures to practices recommended under a number of legal frameworks and national standards, including regulations promulgated under HIPAA and standards for risk management of data security put forth by the National Institute of Standards and Technology. The Commission clarified that while these standards did not control the outcome of the case, in the Commission's view they provided guidance on baseline requirements for reasonable data security.[8]

Unfairness Implications

The Commission's broad claim of authority in this Opinion may make it vulnerable to reversal on appeal. First, the Commission's assertion that embarrassment and reputational harms are independent substantial consumer injuries lacks support in established law and potentially conflicts with the FTC's 1980 Policy Statement on Unfairness (the "1980 Statement"), the agency's description of what it considers to be the scope of its unfairness authority. The 1980 Statement states that subjective harms "will not ordinarily" make a practice unfair, except in "extreme" cases. Even in extreme cases, the 1980 Statement appears to suggest that emotional harms must be coupled with "tangible injury" to justify a finding of unfairness. Nothing in the Commission's Opinion articulates why the potential embarrassment alleged in the LabMD case should be considered "extreme." The example the Commission suggested as a sufficient emotional harm—"harassing late-night telephone calls" from debt collectors—is likely considered more extreme than the emotional harm alleged in this case.

Similarly, the Commission's determination that "likely" means something less than "probable" lacks external support, especially in light of the text of Section 5(n). The Opinion seems to replace the clear statutory requirement of "likely to cause substantial injury," which, by its plain language, requires a probabilistic analysis, with the "significant risk" standard, which seemingly allows a sliding scale approach where the large magnitude of the possible injury can overcome a lower probability the injury will occur. Neither the 1980 Statement, nor the cases cited in the Opinion as precedent (which involved the possibility of *physical* injury) support the Commission's sliding-scale approach in this case.[9]

In addition, the "significant risk" standard potentially conflates the first and third prongs of the Section 5(n) test: the third prong, which requires weighing of the degree of harm against potential benefits to consumers, seems to account for the extent of potential harm, making the analysis of the magnitude of the potential harm in the first prong of the test superfluous.[10]

Moreover, the Commission's analysis was arguably incomplete. The Commission assumed that meeting the three requirements in Section 5(n) is not merely necessary for liability, but also *sufficient*, which is far from clear. Section

[7] The Commission appears not to have analyzed the costs associated with administrative enforcement and remedies in assessing the relative costs and benefits of the practices at issue.
[8] The Commission also rejected arguments by LabMD that it was not provided with fair notice and due process, that certain evidence should have been excluded, and that the Commission followed improper procedures.
[9] Despite the aggressive position staked out in the Commission's opinion, it could have gone much further. The Opinion rejected the argument advanced in the FTC's complaint that any act or practice that creates a "significant risk of concrete harm" in and of itself *causes* a substantial injury for purposes of the Act.
[10] The Commission's focus on whether the practice *"was likely"* to cause injury at the time it was implemented is also inconsistent with the language of the statute, which calls for an analysis of whether the practice "is likely" to cause injury at present.

5(n)'s statutory prerequisites on their face set the *outer bounds* of unfairness,[11] and at least one court has acknowledged that additional requirements for liability may constrain the FTC's authority beyond those listed in Section 5(n).[12]

Order Implications

As the result of its Opinion, the Commission imposed a 20-year remedial order, requiring implementation of a comprehensive information security program, biennial assessments, and recordkeeping and reporting requirements.

While in some ways this Order is typical for an FTC data security case, notably, the FTC entered the Order even though LabMD went out of business in 2014. The Commission justified imposing the Order by arguing that the company still possesses personal information collected prior to shutting down, and could resume operations at any time, once again placing consumer data at risk.

The Order also requires LabMD to notify affected consumers and their health insurers, a provision not usually imposed by the FTC unfairness-based data security orders. LabMD may have a particularly strong argument that this requirement is not reasonably related to the alleged violation, which focused on an absence of reasonable security measures.

Healthcare Implications

The Commission's Opinion also serves as a reminder of the FTC's increasingly aggressive presence in a space more traditionally regulated by OCR and States' Attorneys General.[13] Since announcing in June 2015 that it would assume a more prominent role in regulating "Big Data," the FTC has asserted its jurisdiction over other health care entities, yielding settlements with a cloud-based electronic health records company and a dental practice software provider, in each case concerning data privacy and security.

In the absence of OCR action or input in either of these settlements or the LabMD matter,[14] health care entities may well be wondering how best to ensure compliance with multiple sets of federal and even state standards for data security or, quite possibly, multiple interpretations of a single set of Federal data security standards. Not insignificantly, in its opinion, the Commission referred to the HIPAA Security Rule, among other standards, to provide "a useful benchmark for reasonable behavior" with respect to data security practices and also to inform whether and to what extent LabMD's practices were fair and consistent with industry practice. Certainly, the Commission's interpretation of what HIPAA requires as a "benchmark" may differ from OCR's interpretation and may lead to action by the FTC that OCR did not intend. For example, the HIPAA Security Rule, which the FTC has identified as a "benchmark," was finalized by OCR in 2003 and went into effect in April 2005. By taking enforcement action against LabMD on grounds that "from at least 2005…, LabMD did not have basic data security practices in place for its network" that would "provide reasonable and appropriate security for personal information

[11] *See* 15 U.S.C. § 45(n) ("The Commission *shall have no authority* under this section or section 57a of this title to declare unlawful an act or practice on the grounds that such act or practice is unfair *unless* the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. . . .")

[12] *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 244 (3d Cir. 2015) (stating that the elements enumerated in Section 5(n) may be necessary but insufficient conditions for unfairness liability).

[13] Since the passage of the HITECH Act in 2009 "gave States' Attorneys General the authority to bring civil actions on behalf of state residents for violations of the HIPAA Privacy and Security Rules," state attorneys general have increasingly brought actions against health care entities "to obtain damages on behalf of state residents or to enjoin further violations of the HIPAA Privacy and Security Rules." *See State Attorneys General*, HHS, here.

[14] In its 2013 motion to dismiss the case, LabMD noted it "has never been accused of violating HIPAA or HITECH by the FTC, HHS, or anyone else." Respondent LabMD, Inc.'s Motion To Dismiss Complaint With Prejudice And To Stay Administrative Proceedings, *In the Matter of LabMD, Inc.*, Dkt. No. 9357 at 4, (FTC, Nov. 12, 2013), available here.

stored on its computer network," the FTC is comparing LabMD's previous data practices to a standard that had just recently been created by OCR—perhaps taking away from OCR's discretion in determining how much leeway entities should be given in adjusting to new compliance requirements.

Moreover, if the FTC and OCR were to assert simultaneous jurisdiction over a health care entity's data security, that entity might become subject to two different and even potentially conflicting sets of requirements. The health care industry will need to pay close attention to the interplay between the FTC and OCR in order to identify and address potentially conflicting standards in the security of protected health information.

Finally, the relief sought by the FTC—requiring that LabMD notify affected consumers, establish a comprehensive information security program reasonably designed to protect the security and confidentiality of the personal consumer information in its possession, and obtain independent assessments regarding its implementation of the program—is especially puzzling, given that LabMD is defunct, as mentioned above.

The health care industry should recognize that this decision suggests that more attempted regulation of protected health information by agencies other than OCR is yet to come, and also perhaps increasing enforcement by those agencies as new theories of liability are adopted.

Conclusion

The LabMD case continues to be of significant interest to observers of the FTC's ongoing attempts to expand its authority. It should also be closely followed by all companies potentially at risk of data breach, and particularly those in the health care space. It remains to be seen just what the final outcome will be, but the recent Opinion gives further insight into the Commission's understanding of reasonable data practices and demonstrates its increasing likeliness to aggressively pursue cases, even in the absence of concrete injury.

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, Paul Rubin, David Cohen, or another member of Ropes & Gray's leading privacy & data security team.

For additional information on the OCR HIPAA audit program, please see our HIPAA Audits Resource Center.