haynesboone

September 8, 2016

Full Federal Trade Commission Reverses ALJ, Holds LabMD Liable for Data Breach, but Declines To Decide Whether Lax Data Security Breaches Section 5

By Pierre Grosdidier

In a unanimous opinion written by Chairwoman Edith Ramirez, the Federal Trade Commission ("FTC") reversed an Administrative Law Judge's ("ALJ") decision that had dismissed Section 5 (15 U.S.C. § 45, the "FTC Act") claims against LabMD for an eight-year-old data breach.[1] The FTC held that the ALJ applied the wrong legal standard and ordered now-inactive LabMD to comply with a number of data-protection measures.[2] The importance of the decision is that it helps set the threshold conditions under which the FTC will consider that a data breach, or *the risk of a data breach*, constitutes a Section 5 violation.

Section 5 of the FTC Act bars "unfair or deceptive acts or practices in or affecting commerce" and authorizes the FTC to police such conduct.[3] But the FTC's authority is restricted to acts that, *inter alia*, cause or are "likely to cause substantial injury to consumers."[4] The FTC has used the FTC Act to police companies whose inadequate or ineffective security measures have resulted in data breaches and, consequently, consumer harm.[5]

The account of the FTC's proceeding against LabMD is convoluted and controversial. LabMD was a medical testing services company that unwittingly granted public access via peer-to-peer software to a large file (the "1718 File") that contained the Personally Identifiable Information ("PII") of some 9,300 patients, including social security numbers and medical data. The FTC filed a complaint against LabMD after Tiversa, Inc., a third-party, found the 1718 File and turned it over to the FTC under contentious circumstances. The ensuing polemic led to a Congressional inquiry and report that cast the FTC and Tiversa in an unflattering light.[6] LabMD eventually unwound its operations in 2014, and the FBI raided Tiversa in March 2016.[7]

The Commission found that the record supported FTC Complaint Counsel's claim that LabMD's data security measures fell substantially short of minimum established norms, especially for a facility that housed medical PII for over 750,000 patients.[8] Unauthorized access protection was very weak and security audits lackadaisical. At least six employees used the password "labmd," for example, and LabMD's IT services failed to detect the peer-to-peer software until the breach occurred. But the record also shows that only

---

[1] Opinion of the Commission, *In re LabMD, Inc*., FTC No. 9357 (July 29, 2016) [hereinafter "Commission Opinion"). The *In re LabMD* pleadings are available here. *See also* Pierre Grosdidier, *Speculative Data Breach Damages Might Be Actionable*, excerpted from State Bar of Texas, Computer and Technology Section's Circuits Newsletter, May 2016, available here.

[2] Final order, *In re LabMD, Inc.*, FTC No. 9357 (July 28, 2016).

[3] 15 U.S.C. § 45(a)(1)—(2).

[4] *Id.* § 45(n).

[5] Commission Opinion at 10 n.21 ("[t]o date, using both its deception and unfairness authority, the Commission has brought nearly 60 data security cases.").

[6] *Tiversa, Inc.: White Knight or Hi-Tech Protection Racket?*, Comm. on Oversight and Gov't Reform, U.S. House of Rep., 113th Cong. (Jan. 2, 2015) ("Committee Report").

[7] http://www.theregister.co.uk/2016/03/18/fbi_raids_cybersecurity_firm_tiversa/.

[8] Commission Opinion at 11-16.

Tiversa accessed the 1718 File and no one ever complained, or presented evidence, of a tangible injury because of the data breach.[9]

In its action against LabMD, Complaint Counsel took the position, *inter alia*, that a company's lax computer security measures are actionable under the FTC Act even in the absence of a data breach.[10] According to this argument, Section 5 liability can be imposed merely based on the risk that inadequate security measures will cause a data breach resulting in future consumer harm.[11] In its Initial Decision dismissing the FTC's complaint, the Administrative Law Judge ("ALJ") specifically rejected this argument because it required too many speculative steps between the lax security and actual consumer harm. In dismissing Complaint Counsel's claim regarding the 1718 File, the ALJ also held that "Complaint Counsel ha[d] proven the 'possibility' of harm, but not any 'probability' or likelihood of harm."[12]

In reversing the ALJ, the Commission held that the release of the 1718 File, which contained sensitive personal medical information, caused sufficient consumer injury to satisfy the Section 5 threshold.[13] This was so even though only Tiversa accessed the 1718 File. The Commission also held separately that the exposure of the 1718 File for 11 months on a peer-to-peer file-sharing site was in and of itself actionable under Section 5 because it created a "significant risk" of substantial consumer injury.[14] The unauthorized release of one file containing PII to one party is, therefore, actionable under Section 5, as is publicly exposing such a file through peer-to-peer software, even in the absence of evidence of actual copying.

But, significantly, the Commission expressly declined to address Complaint Counsel's "broader argument" that inadequate security measures that potentially expose PII to a breach constitute a Section 5 violation in and of themselves:

> We note that Complaint Counsel argues that LabMD's security practices risked exposing the sensitive information of all 750,000 consumers whose information is stored on its computer network and therefore that they create liability even apart from the LimeWire incident. We find that the exposure of sensitive medical and personal information via a peer-to-peer file-sharing application was likely to cause substantial injury and that the disclosure of sensitive medical information did cause substantial injury. Therefore, we need not address Complaint Counsel's broader argument.[15]

The Commission, therefore, saw no need to opine on Complaint Counsel's most reaching argument. However, companies that host large quantities of PII would be ill-advised to find solace in the Commission's restraint, given the zeal that the FTC showed in policing the LabMD breach. This is especially so considering the ever-growing sophistication of hackers which, arguably, constantly shifts what constitutes a "significant risk" of data breach and, therefore, consumer injury. Meanwhile, the controversy continues: LabMD has already stated its intent to appeal the Commission's decision to a Court of Appeals.[16]

---

[9] Tiversa also shared the 1718 File with an academic researcher.

[10] Complaint Counsel's Appeal Brief, *In re LabMD, Inc.*, FTC No. 9357, at 5-7, 10-12 (Dec. 22, 2015).

[11] Initial Decision, *In re LabMD, Inc., FTC No. 9357, at 84—85 (Nov. 13, 2015).*

[12] Initial Decision at 14.

[13] Commission Opinion at 17-19.

[14] *Id.* at 20-25.

[15] *Id.* at 16.

[16] Allison Grande, *FTC Revives LabMD Data Leak Suit, Finds Consumer Harm*, Law360 (July 29, 2016).