June 12, 2018

Eleventh Circuit Vacates FTC Cease and Desist Order for Failing to Enjoin Specific Cybersecurity Lapses

Court Holds FTC Must Articulate Specific Cybersecurity Measures to Be Implemented

SUMMARY

On June 6, 2018, in the closely watched case *LabMD, Inc.* v. *Federal Trade Commission*,[1] the Eleventh Circuit Court of Appeals vacated a cease and desist order (the "Order") issued by the Federal Trade Commission (the "FTC") that would have required LabMD, Inc. ("LabMD") to, among other things, "establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers." Sidestepping the central question of whether the FTC has authority to regulate alleged cybersecurity deficiencies under its unfairness jurisdiction in the absence of tangible consumer harm, the Eleventh Circuit held that, because the Order failed to enjoin any specific act or practice and instead "command[ed] LabMD to overhaul and replace its data-security program to meet an indeterminable standard of reasonableness," the Order was insufficiently specific and therefore unenforceable.

BACKGROUND

LabMD is a now-defunct medical testing laboratory that previously used medical specimen samples, along with relevant patient information, to assist physicians in making diagnoses. LabMD stored sensitive information concerning approximately 750,000 patients on its computer networks, including patients' names, dates of birth, Social Security numbers, laboratory test codes, test results, and health insurance information. As a result, LabMD was subject to data security regulations issued under the Health

Insurance Portability and Accountability Act of 1996 ("HIPAA"), and maintained a data security program in an effort to comply with those regulations.

In 2005, contrary to LabMD's policy, a peer-to-peer ("P2P") online file-sharing program was installed on a LabMD employee's computer and certain files were designated for sharing with other program users. While most were music and video files, between July 2007 and May 2008, a 1,718-page file (the "1718 File") containing medical and other sensitive personal information of approximately 9,300 consumers was inadvertently designated for sharing.[2] After a third-party data security firm downloaded the 1718 File through the program, alerted LabMD, and offered remediation services, LabMD discovered the program on the employee's computer and promptly removed it. The data security firm informed the FTC of the incident.

In August 2013, after conducting an investigation, the FTC issued an administrative complaint against LabMD alleging that LabMD failed to employ reasonable and appropriate data security measures to prevent unauthorized access to its computer networks. While the focal point of the FTC's complaint was the unauthorized installation of the P2P program and exposure of the 1718 File, the complaint broadly alleged that LabMD had "engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on its computer networks";[3] that these failures caused or were likely to cause substantial injury to consumers; and that they therefore amounted to an "unfair act or practice" prohibited by Section 5(a) of the Federal Trade Commission Act of 1914 (the "Act").

On November 13, 2015, an Administrative Law Judge (the "ALJ") dismissed the FTC's complaint, finding that the disclosure of the 1718 File did not constitute an "unfair act or practice" because it is unlikely that the disclosure "cause[d] or [wa]s likely to cause substantial injury to consumers," as required by Section 5(n) of the Act.[4] The ALJ found that there was minimal risk of any harm to consumers given the lack of evidence that any consumer listed in the 1718 File had suffered harm or that anyone other than the data security firm had downloaded the file. Moreover, the ALJ found there was insufficient evidence that the file's exposure was likely to cause reputational or emotional harm, and that, in any event, any such subjective harm (including privacy harm) does not, standing alone, constitute "substantial injury" within the meaning of Section 5(n).

The FTC appealed the ALJ's decision to the full Commission, which reversed the decision in a July 29, 2016 Opinion and Final Order. The FTC determined that LabMD's data security practices, which lacked "basic" safeguards, were unfair within the meaning of Section 5 of the Act.[5] These deficiencies, the FTC concluded, were unreasonable and permitted the installation of the P2P program and the eventual exposure of the 1718 File. The FTC also held that the unauthorized exposure of the 1718 File for more than 11 months through the P2P program was "likely to cause substantial injury" and did, in fact, cause real privacy harm given that sensitive health information was exposed. Expressly disagreeing with the

ALJ, the FTC concluded that privacy harm, standing alone, can constitute "substantial injury" under Section 5(n) even in the absence of tangible economic or physical injury.

The FTC entered the Order, which was meant to "ensure LabMD reasonably protects the security and confidentiality of the personal consumer information in its possession."[6] Pursuant to the Order, LabMD was required to:

> establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers . . . . Such program . . . shall contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers . . . .[7]

LabMD was further required to obtain periodic, independent assessments regarding the implementation and effectiveness of the program for a period of 20 years, and notify those consumers and their health insurance companies whose personal information had been exposed through the P2P program.

LabMD petitioned the Eleventh Circuit for review, arguing that, pursuant to Section 5(n), intangible harms (such as reputational and privacy harms) could not alone constitute "substantial injury" and that a practice could not be "likely" to cause substantial injury where the "likelihood of the injury occurring is low."[8] LabMD further argued that it lacked fair notice of the FTC's interpretation of Section 5(n) as required by the Due Process Clause; that the FTC's Opinion was not supported by substantial evidence; and that the Order's remedies were improper on the alleged grounds that there was no cognizable risk of the defunct company committing the purported violation again, the Order consisted entirely of affirmative relief that the FTC lacks authority to impose, and the Order was impermissibly vague. The Eleventh Circuit stayed the Order pending resolution of the appeal.

THE ELEVENTH CIRCUIT'S DECISION

The Eleventh Circuit vacated the FTC's Order on the narrow issue of enforceability, finding that the Order was insufficiently specific to be enforceable. The Eleventh Circuit did not reach the question as to whether the failure to implement and maintain a reasonable data security program where no tangible consumer injury results can constitute an unfair act or practice under Section 5(a) of the Act. The court expressly rejected the view that the FTC "may bring suit purely on the basis of substantial consumer injury," holding instead that for an act or practice to be "unfair," in addition to meeting the "substantial injury" requirements of Section 5(n), the act or practice's "unfairness" must be "grounded in well-established legal policy," such as in statute, the common law, or the Constitution.[9] The court then turned to two questions raised by LabMD's petition for review: (a) "whether LabMD's failure to implement and maintain a reasonably designed data-security program constituted an unfair act or practice within the

ambit of Section 5(a)"; and (b) "whether the [FTC]'s cease and desist order, founded upon LabMD's general negligent failure to act, is enforceable."[10]

As to the "ground[ing] in well-established legal policy," the court noted that while the FTC's Opinion "does not explicitly cite the source of the standard of unfairness it used," "[i]t is apparent . . . that the source is the common law of negligence."[11] The court reasoned that the "gist" of the FTC's complaint and decision was that consumers' right of privacy is protected against unintentional invasion and that companies that negligently invade that right can be held accountable under Section 5(a) of the Act.[12]

The court declined to decide the question whether LabMD's alleged failure to implement and maintain a reasonably designed data security program constituted an unfair act or practice within the ambit of Section 5(a). Instead it assumed *arguendo* that the FTC was correct that such an alleged failure "invaded consumers' right of privacy and thus constituted an unfair act or practice" subject to the FTC's authority.[13]

Turning to the final question—the enforceability of the FTC's Order—the court determined that the Order was insufficiently specific to be enforceable because it listed no specific unfair acts or practices in which LabMD had to desist engaging, instead mandating "a complete overhaul of LabMD's data-security program" while saying "precious little about how this is to be accomplished."[14] While affirming the FTC's authority to develop the meaning of "unfairness" through case-by-case litigation (in addition to formal rule-making), the court stressed that, to address due-process concerns, the FTC's complaints and resulting remedies must be specific, clear, and precise with respect to the prohibited acts or practices. This, the court explained, is true regardless of whether the remedy takes the form of a cease and desist order issued by an administrative law judge, or an injunction issued by a district court. The court noted that insufficiently specific orders lead to meaningful enforcement challenges and impermissibly put courts "in the position of managing [a company's] business in accordance with the [FTC's] wishes."[15] Under this standard, the court concluded that the Order was unenforceable because it was "devoid of any meaningful standard informing the court of what constitutes a 'reasonably designed' data-security program."[16]

In dicta, the court also appeared to chastise the FTC for the sweeping nature of its complaint against LabMD, noting that the FTC used the installation of the P2P program on a computer and the ensuing exposure of the 1718 File "as an entry point to broadly allege that LabMD's data-security operations are deficient as a whole," despite the fact that "[a]side from the installation of [the P2P program] . . . , the complaint alleges no specific unfair acts or practices engaged in by LabMD."[17] The court suggested that, had the FTC's Complaint instead narrowly focused on the installation of the P2P program in defiance of LabMD policy, "a narrowly drawn and easily enforceable order might have followed, commanding LabMD to eliminate the possibility that employees could install unauthorized programs on their computers."[18]

The FTC has not yet indicated whether it will seek to challenge the ruling, which it can do through a petition to the Eleventh Circuit for rehearing *en banc* or to the U.S. Supreme Court.

IMPLICATIONS

Although the Eleventh Circuit did not decide the most closely followed question raised in LabMD's appeal—whether the FTC has authority to prosecute alleged inadequate data security practices in the absence of tangible consumer harm—the decision may nonetheless have significant consequences both in data security cases and beyond. The decision indicates that in future enforcement actions, the FTC must set forth both (a) specific allegations and proposed remedies relating to particular allegedly "unfair" data security or other deficiencies and (b) a statutory or legal basis for finding such deficiencies "unfair." At least in the Eleventh Circuit, companies may now insist that the FTC articulate specific data security requirements in consent orders, and administrative law judges and district courts issuing and enforcing FTC cease and desist orders and injunctions will likely require the FTC to set out more specific data security standards against which to ascertain compliance.

The Eleventh Circuit's decision may also lead potentially to enforceability challenges to FTC and other agency-issued cease and desist orders more generally. Such orders, routinely issued in a wide variety of contexts, often require that the respondent create or enhance compliance programs to the agency's satisfaction for consumer protection, anti-money laundering, or other regulatory compliance activities. Notably, the general "reasonableness" language to which the Eleventh Circuit objected in the vacated Order—which required the implementation and maintenance of "a comprehensive information security program that is reasonably designed to protect the security and confidentiality of consumers' personal information"[19]—is reflected in numerous FTC orders. Similarly broad language is likewise found in orders issued by other agencies that have similar authority to prohibit unfair or deceptive practices, including the BCFP (formerly called the Consumer Financial Protection Bureau), the federal banking agencies, and state attorneys general pursuant to states' "mini-FTC" statutes. To the extent such affirmative prospective requirements are not accompanied by a more precise description of the particular acts or practices that must be avoided, or sufficient detail regarding the actions that must be undertaken to ensure compliance, they may well be challenged by companies as unenforceable under the Eleventh Circuit's reasoning in *LabMD*.

While the Eleventh Circuit sidestepped the question of the FTC's authority to regulate data security practices in the absence of alleged tangible customer harm, statements by the new chair of the FTC during his February 2018 confirmation hearing indicate that, going forward, the FTC will decline to bring enforcement actions in these circumstances and will instead prioritize consumer protection issues "where [consumer] harm is the greatest."[20]

LabMD is unlikely to alter the FTC's view that it may generally regulate data security practices under its "unfairness" authority. In its July 29, 2016 Opinion, the FTC noted that it has "long challenged under its unfairness authority . . . unreasonable and inappropriate data security practices"[21] and that the FTC has

brought nearly 60 data security cases pursuant to its authority to regulate unfair or deceptive acts or practices under Section 5(a) of the Act.[22]

The FTC may also be expected to continue taking a contextual approach to assessing companies' data security programs, with the "touchstone" of that approach being "reasonableness."[23] Although the Eleventh Circuit criticized the lack of specificity in both the FTC's complaint and Order regarding what practices would be "reasonable," the FTC nonetheless identified in its Opinion certain specific security measures it considers "basic": automated intrusion detection systems and file integrity monitoring software to assess risks and identify suspicious activity, penetration testing to identify vulnerabilities that can be exploited to obtain unauthorized access, and monitoring of networks for unauthorized intrusions or exfiltration.[24] Given the Eleventh Circuit's endorsement of the FTC's case-by-case rule-making authority, companies would do well to ensure that, to the extent appropriate based on the particular cyber risks they face, such measures form part of their cybersecurity program. Likewise, companies should look to FTC consent decrees in other data security cases to inform their assessment of the reasonableness of their data security practices. Helpfully, in June 2015, the FTC released a Guide for Businesses setting out 10 practical lessons for businesses distilled from more than 50 of the FTC's data security settlements, including in areas such as access rights to data and networks, storage and transmission of sensitive personal information, and procedures to maintain up-to-date security programs and address vulnerabilities.[25]

* * *

ENDNOTES

1 No. 16-16270 (11th Cir. June 6, 2018) (Opinion).

2 *Id*. at 3.

3 *Id.* at 14.

4 15 U.S.C. § 45(n).

5 *LabMD, Inc.*, Docket No. 9357 (FTC July 29, 2016) at 1-2 (FTC Opinion).

6 *Id.* at 34.

7 *Order*, at 2.

8 The FTC held 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." FTC Opinion, at 10.

9 Opinion, at 13.

10 *Id.* at 16, 18.

11 *Id.* at 16-17.

12 *Id*. at 17.

13 *Id.* at 17-18.

14 *Id.* at 30-31.

15 *Id.* at 30.

16 *Id*. at 29. Although the court focused its decision on the first provision in the Order, which required LabMD to "establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers," it noted that the Order's other provisions regarding LabMD's data security program were equally vague and unenforceable. These required LabMD to, among other things, designate an employee to coordinate its information security program; conduct a risk assessment; design and implement "reasonable" safeguards to control risks identified through the risk assessment; regularly test or monitor the safeguards' effectiveness; develop and use "reasonable" steps in the selection and retention of service providers; and evaluate and adjust LabMD's information security program in response to monitoring and testing results and material changes. *See* Order, at 2-3.

17 Opinion, at 14.

18 *Id*.

19 *Id.* at 34.

20 Hamza Shaban, "Nominee for FTC chairman signals scrutiny for tech giants," *The Washington Post* (February 14, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/02/14/nominee-for-ftc-chairman-signals-scrutiny-for-tech-giants/.

21 FTC Opinion, at 10.

22 *Id*. at 10.

23 *Id.* at 11.

24 *Id*. at 11-13.

25 *See* Start with Security: A Guide for Business, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers listed below, or to any other Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.

CONTACTS

New York		
H. Rodgin Cohen	+1-212-558-3534	cohenhr@sullcrom.com
Mitchell S. Eitel	+1-212-558-4960	eitelm@sullcrom.com
John Evangelakos	+1-212-558-4260	evangelakosj@sullcrom.com
Nicole Friedlander	+1-212-558-4332	friedlandern@sullcrom.com
Scott D. Miller	+1-212-558-3109	millersc@sullcrom.com
Nader A. Mousavi	+1-212-558-1624	mousavin@sullcrom.com
Alexander J. Willscher	+1-212-558-4104	willschera@sullcrom.com
Michael M. Wiseman	+1-212-558-3846	wisemanm@sullcrom.com
Washington, D.C.		
Eric J. Kadel, Jr.	+1-202-956-7640	kadelej@sullcrom.com
Stephen H. Meyer	+1-202-956-7605	meyerst@sullcrom.com
Jennifer L. Sutton	+1-202-956-7060	suttonj@sullcrom.com
Samuel R. Woodall III	+1-202-956-7584	woodalls@sullcrom.com
Palo Alto		
Scott D. Miller	+1-650-461-5620	millersc@sullcrom.com
Nader A. Mousavi	+1-650-461-5660	mousavin@sullcrom.com