Christopher Fonzone Partner
cfonzone@sidley.com
Kate Heinzelman Counsel
kheinzelman@sidley.com
Sidley Austin LLP, Washington DC

After *LabMD*, questions remain for the healthcare sector

Massive data breaches. Threats to medical devices. The Internet of Persons. Healthcare entities are all too familiar with the rising cyber threat. But they are also familiar with the complex array of laws and regulations in the United States that attempt to address the threat and the potentially significant compliance costs and risks caused by that complexity. The US Court of Appeals for the Eleventh Circuit's recent and long-awaited decision in *LabMD v. Federal Trade Commission*, which trimmed the sails of one of the primary regulators of the healthcare information security landscape, may thus appear to some, at first blush, to be a necessary corrective. Yet closer inspection shows that the Eleventh Circuit's decision raises more questions than it answers - and that its true implications will only become clear once we see how federal regulators, the courts, and perhaps Congress respond, as Christopher Fonzone and Kate Heinzelman of Sidley Austin LLP explain.

The regulatory landscape

The fact that multiple regulators play a role in regulating aspects of health information security in the United States has drawn policy attention in recent years. For instance, a year ago, the congressionally mandated Health Care Industry Cybersecurity Task Force discussed the US federal and state regulatory landscape for healthcare cyber security in its Report on Improving Cybersecurity in the Health Care Industry. Noting that "health care cybersecurity is a key public health concern that needs immediate and aggressive attention[1]," the Task Force called for streamlining and reform. "While many regulations that apply to cybersecurity in health care are well-meaning and individually effective," the Task Force argued, "taken together they can impose a substantial legal and technical burden on health care organizations[2]." This is because, the report continued, the current regulatory environment requires healthcare entities to "continually review and interpret multiple regulations, some of which are vague, redundant, or both[3]."

Policy questions aside, as we explain further below, the *LabMD* litigation raises a related legal question about the significance of these multiple regulatory regimes. Although this short article cannot detail the entire regulatory environment, the litigation implicates two of the most important federal regulatory frameworks, discussed here in turn:

The Department of Health and Human Services ('HHS')

The Health Insurance Portability and Accountability Act of 1996 and its implementing regulations, as amended by the Health Information Technology for Economic and Clinical Health Act (collectively referred to as 'HIPAA'), are, of course, well known to healthcare entities. HHS enforces HIPAA though its Office for Civil Rights ('OCR'), holding companies to a variety of rules for protecting patients' health information. These rules, among other things, limit healthcare entities' ability to disclose individually identifiable health information; direct entities to implement appropriate administrative, physical, and technical safeguards; and mandate covered entities to notify individuals and the HHS of breaches of protected information. Most relevantly here, the HIPAA 'Security Rule' requires companies to put in place appropriate information security safeguards but does not 'mandate particular technical solutions[4].' Finally, should the OCR find an entity to be non-compliant with its HIPAA obligations, including the 'Security Rule,' it typically attempts to resolve the issue through voluntary compliance, corrective actions, or resolution agreements.

The Federal Trade Commission ('FTC')

The FTC is another primary information security regulator. Unlike the HHS, however, the FTC largely does not regulate by enforcing a health and privacy specific statutory scheme like HIPAA[5]. Rather, over the last two decades, the FTC has relied on Section 5(a) of the Federal Trade Commission Act to hold companies accountable for 'unfair or deceptive' information security 'acts or practices[6].' Enforcement actions brought pursuant to this authority have, among other things, targeted companies - including healthcare companies - for failing to take basic security steps, and the FTC often remediates these violations by requiring companies to put in place a comprehensive information security program reasonably designed to protect personal information.

The *LabMD* case

These enforcement regimes form the backdrop for *LabMD*, a case with a history that rivals *Jarndyce v. Jarndyce,* such that we can provide only a brief summary of the facts and procedural background here.

In February 2008, a data security research company used a peer-to-peer file sharing system to download a file containing consumers' protected information from LabMD, a medical laboratory no longer in operation. A LabMD employee had, contrary to company policy, installed the file sharing system on his computer. Once made aware of this, LabMD removed the system from the employee's computer, but the FTC, after learning of the breach, nonetheless filed a complaint in 2013 alleging that LabMD's data

Although the Court did not explain why it took this approach, one possible hypothesis is that the Court was concerned with the FTC's claim of authority, but did not want to create a square split with the Third Circuit on this issue.

continued

security program was inadequate and thus constituted an 'unfair act or practice' under the FTC Act.

This complaint launched years of litigation, as LabMD repeatedly sought to enjoin the FTC proceedings on the ground that the FTC exceeded its statutory authority and unconstitutionally deprived LabMD of sufficient notice in bringing its enforcement action. The Eleventh Circuit twice refused such challenges on the ground that the FTC should be given a chance to consider LabMD's claims in the first instance, and LabMD voluntarily dismissed a similar action in the US District Court for the District of Columbia[7]. The case thus proceeded to trial before an administrative law judge, who agreed with LabMD and dismissed the complaint on the ground that the FTC failed to prove that LabMD's cyber security practices caused or were likely to cause harm to consumers. The FTC ultimately reversed, however, and issued an order requiring 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. [. . .] 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."

The Commission concluded, among other things, that "the privacy harm resulting from the unauthorized disclosure of sensitive health or medical information is in and of itself a substantial injury under Section 5(n)," and that "LabMD's sharing of the [file] on [the file sharing system] for 11 months was [. . .] highly likely to cause substantial privacy harm to thousands of consumers, in addition to the harm actually caused by the known disclosure[8]." LabMD immediately challenged the order, the Eleventh Circuit stayed the FTC's ability to enforce it pending judicial review[9], and the case mentioned at the outset ensued.

The Eleventh Circuit's decision

In its briefing to the Eleventh Circuit, LabMD advanced numerous arguments, three of which are worth discussing here.

Preemption

First, LabMD argued that the Commission should not be able to enforce Section 5(a) against LabMD because Congress had delegated to the HHS - and not the FTC - "broad discretion" to set "comprehensive standards" for data security in the healthcare industry under HIPAA[10]. LabMD asserted that it complied with HIPAA, and that this was the reason the HHS had not joined the FTC's action[11]. The FTC's Complaint Counsel disputed before the Commission the basis for LabMD's assertion and argued that it did not matter, in any event, because it was enforcing the FTC Act, not HIPAA[12]. Before the Appeals Court, the FTC argued that HIPAA in no way preempts its authority to bring enforcement actions against "unfair or deceptive acts or practices" under Section 5(a) of the FTC Act, since there is "no conflict, or even potential conflict" between the two statutes[13]. Moreover, the FTC noted, there can be no argument that HIPAA occupies the field, as a variety of other laws, such as the Fair Credit Reporting Act and the Freedom of Information Act, specifically cover medical information[14].

Perhaps unsurprisingly, the Eleventh Circuit chose to sidestep this issue. While noting that LabMD "employed a data-security program in an effort to comply with [HIPAA] regulations," the Court declined to comment on LabMD's preemption argument - instead resolving the dispute on other grounds.

Authority

LabMD's second major argument was that the FTC's actions in this case exceeded the Commission's Section 5 authority, since it was insufficiently "clear and well-established" that LabMD's conduct was "unfair" under the FTC Act. In advancing this argument, LabMD's claims mirrored a consistent line of criticism leveled against the FTC[15], although the only Court of Appeals to address the issue before the Eleventh Circuit, the Third Circuit, had decisively ruled that the FTC does have the authority to regulate "unfair" data security practices[16].

This prior Court of Appeals decision may explain the Eleventh Circuit's unusual treatment of this issue. To begin its analysis of LabMD's claim, the Court noted that the "Commission must find the standards of unfairness it enforces

in 'clear and well-established' policies that are expressed in the Constitution, statutes, or the common law" and then stated that the Commission had failed to cite explicitly the source of the unfairness standard it applied to LabMD. The Court continued, however, by concluding that it is "apparent" that the Commission's unstated "source is the common law of negligence," and, in particular, the protection against an unintentional invasion of privacy[17]. But before carrying this theme through to its logical conclusion - by addressing whether it is sufficiently well-established that "deficient data-security" can constitute actionable negligence - the Court simply assumed for the sake of argument that it could. In other words, the Court engaged in a substantive discussion of the FTC's unfairness authority before rendering its entire analysis of the issue non-binding *dicta*.

Although the Court did not explain why it took this approach, one possible hypothesis is that the Court was concerned with the FTC's claim of authority, but did not want to create a square split with the Third Circuit on this issue[18]. Another is that the Eleventh Circuit may have thought that the ground on which it ultimately resolved the case - enforceability, discussed next - was narrower and therefore less disruptive to the FTC's mission. But, as described further on, and as one of us has discussed previously in analysing the case, if these were the concerns underlying the Court's approach, it may not have picked the best way to achieve them[19].

Enforceability

As noted above, the Eleventh Circuit agreed with LabMD's final argument, that the FTC's order was "unenforceable" because it did not define with enough specificity what sort of conduct it prohibited. The Eleventh Circuit pointed to several factors in reaching this conclusion. First, the Court noted that the FTC Act authorises the Commission to define rules "which define with specificity" what constitutes unfair activity under Section 5[20]. Second, the Court pointed to half-century old Supreme Court precedent for the proposition that it may violate due process to impose penalties for violations of an imprecise cease-and-desist order[21].

Finally, the Court noted that, were it faced with a factual dispute over whether LabMD had put in place a "'reasonably-designed' data-security program," it would have "no choice but to conclude that the Commission has not proven - and indeed cannot prove - LabMD's alleged violation by clear and convincing evidence," which is the quantum of proof for a Court to uphold a contempt order[22], given that the order "is devoid of any meaningful standard informing the court of what constitutes a 'reasonably designed' data-security program." The Court accordingly concluded that the FTC's order was unenforceable.

What does it mean?

Although the Court may have thought that enforceability was a narrower ground for a decision than limiting the FTC's inherent authority, as one of us has previously noted, the order at issue in *LabMD* is not unlike many of the FTC's cyber security orders, which typically require a company to put in place an information security program that is reasonably designed to protect the security, confidentiality, and integrity of consumer personal information[23]. Moreover, other regulatory regimes use similar formulations in describing information security requirements. Consider, for instance, the cyber security directives promulgated under the Gramm-Leach-Bliley Act. Indeed, the Commission's directive that LabMD implement a comprehensive information security program including specified elements is consistent with the elements of such a program that the FTC specified in its Safeguards Rule implementing the Gramm-Leach-Bliley Act[24]. Even if the Court did not intend for them to be, the consequences of the Eleventh Circuit's decision are therefore potentially far-reaching[25].

How far-reaching, however, will depend on what happens next. First, the FTC will have to decide whether it should ask the Eleventh Circuit to hear the case *en banc* or seek *certiorari* from the Supreme Court. The FTC might argue that the Supreme Court should take up the issue to resolve a split between the Eleventh Circuit's decision and the Third Circuit's in *Wyndham*[26] - to say nothing of the internal tension in the Eleventh Circuit's opinion between recognising that the FTC's action was grounded in the venerable common law of negligence, but still nonetheless insufficiently precise to be enforceable.

continued

Further review, however, carries with it substantial risks for the FTC - and potentially other enforcement agencies[27]. The impact of the Eleventh Circuit's decision is geographically constrained in a way that a Supreme Court decision would not be, to say nothing of the fact that the Court could potentially address issues beyond enforceability, such as the scope of the FTC's Section 5 unfairness authority. The FTC - perhaps in cooperation with other enforcement agencies, such as the HHS - may thus be thinking whether there are other ways to address the Eleventh Circuit's decision.

For example, would an enforcement order be sufficiently precise if it referred to a cyber security framework, such as the one promulgated by the National Institute of Standards and Technology[28]? Or might a different approach, such as requiring companies to report back after conducting risk assessments, achieve similar ends[29]? At least in the short term, might the decision result in pressure to shift certain enforcement efforts that the FTC might have otherwise undertaken to other federal information security regulatory regimes, HIPAA included?

Given congressional interest in the subject, the Eleventh Circuit's decision may also prompt Congress to act. As one of us noted previously, while numerous federal and state regulators are increasingly addressing cyber security, Congress has thus far primarily directed its cyber security legislation at encouraging better information sharing[30]. It is thus unclear what Congress would do, even if it did decide that *LabMD* forced its hand: Would it simply restore and potentially clarify the FTC's authority? Would it take a sector-specific approach, for instance, by taking on the healthcare sector and attempting to define further the authorities that operate in this space or centralise cyber security coordination, as the Health Care Industry Cybersecurity Task Force recommended[31]? Or would it pass broad information security legislation that cuts across industries? Only time will tell the answer to these - and the many other - questions raised by the Eleventh Circuit's decision.

1. Health Care Industry Cybersecurity Task Force released its Report on Improving Cybersecurity in the Health Care Industry 2 (June 2017), available at https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf
2. Ibid. at 12.
3. Ibid.
4. HHS, Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA at 16, available at https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf ('A key concept in applying the Security Rule is that it is scalable and flexible to allow implementation of the standards as appropriate for the entity's size, complexity, and capabilities, including its technical, hardware, and software infrastructure.')
5. There is at least one narrow exception. In the Health Information Technology for Economic and Clinical Health Act ('HITECH') Act, enacted in 2009, Congress granted the FTC specific authority to implement a breach notification rule applicable to non-HIPAA covered vendors of personal health records (or 'PHRs'), entities that interact with PHRs, and PHR service providers. See 42 U.S.C. § 17937. Congress specified that violations of the HITECH Act's requirements regarding breach notification for PHRs and their third party service providers would be treated as unfair or deceptive acts or practices in violation of FTC's rules. Ibid. § 17937(e). These particular authorities were not, however, at issue in LabMD, and they are scheduled to sunset should Congress enact new breach notification requirements applicable to non-HIPAA covered entities.
6. See 15 U.S.C. § 45(a).
7. See Lab MD, Inc. v. FTC, 776 F.3d 1275 (11th Cir. 2015).
8. In re LabMD, Inc., Docket No. 9357, at 19, 25 (July 29, 2016), available at https://www.ftc.gov/system/files/documents/cases/160729labmd-opinion.pdf
9. See Lab MD, Inc. v. FTC, 678 Fed. Appx. 816 (11th Cir. 2016).
10. Pet'r's Br. 36 (Dec. 27, 2016).
11. Resp't LabMD, Inc.'s Corrected Answering Br. at 16-17, In re LabMD, Inc., Docket No. 9357 (Feb. 5, 2016).
12. Complaint Counsel's Reply Br. to Resp't's Answering Br. at 6, In re LabMD, Inc., Docket No. 9357 (Feb. 23, 2016).
13. FTC Br. 42 (Feb. 9, 2017).
14. Ibid. at 29-30. Interestingly, the FTC's opinion below referred to HIPAA's requirements as providing "a useful benchmark for reasonable behavior," while noting that they "do not govern whether LabMD met its obligations under Section 5 of the FTC Act." In re LabMD, Inc., Docket No. 9357, at 12 (July 29, 2016).
15. Edward R. McNicholas, Andrew J. Strenio, Jr., Clayton Northouse & Dean C. Forbes, FTC Enforcement of Privacy and Data Security, 500 Privacy & Data Security Practice Portfolio Series, at 225 (Bloomberg BNA).
16. See FTC v. Wyndham Worldwide Corp, 799 F.3d 236 (3d Cir. 2015).
17. In discussing its interpretation of the 'likely to cause' standard in Section 5, the Commission had noted that the Wyndham decision had, like the Commission in this case, "focus[ed] on both the probability and expected size of consumer harm," In re LabMD, Inc., Docket No. 9357, at 21 (July 29, 2016) (internal quotation marks omitted), noting that this standard "is consistent with the standard applied in negligence cases." Ibid. It also noted in response to LabMD's challenge that it lacked adequate notice of the Commission's standards: "it is well-established that the common law of negligence does not violate due process simply because the standards of care are uncodified." Ibid. at 30 (internal quotation marks omitted).
18. Interestingly, one of the three judges on the Eleventh Circuit panel was a judge from the US District Court for the Eastern District of Pennsylvania, sitting by designation. The Eastern District of Pennsylvania is part of the Third Circuit.
19. One of us, along with several of our colleagues, has previously analysed the LabMD decision. We draw upon that analysis throughout. See Timothy J. Muris, Alan Charles Raul, Cameron F. Kerry, Christopher Fonzone, Colleen Theresa Brown & Elizabeth MacGill, 11th Circuit Vacates LabMD Enforcement Order; Casts Doubt on Decades of FTC Cybersecurity Enforcement Practices (June 12, 2018), https://datamatters.sidley.com/11th-circuit-vacates-labmd-enforcement-order-casts-doubt-on-decades-of-ftc-cybersecurity-enforcement-practices/ (hereinafter 'Data Matters Blog').
20. See 15 U.S.C. § 57a.
21. See, e.g., Int'l Longshoremen's Ass'n, Local 1291 v. Phila. Marine Trade Ass'n, 389 U.S. 64, 76, (1967); FTC v. Colgate-Palmolive Co., 380 U.S. 374, 392 (1965).
22. See, e.g., McGregor v. Chierico, 206 F.3d 1378, 1383 (11th Cir. 2000).
23. See Data Matters blog, supra.
24. See 16 C.F.R. § 314.4 (defining the elements of an information security program).
25. Interestingly, the Court could have avoided the Third Circuit's Wyndham decision - and decided the case on what would almost certainly have been a narrower ground - by focusing on whether LabMD's acts were "likely to cause substantial injury to consumers," an issue it discussed in its opinion granting LabMD's stay pending appeal. See Lab MD, Inc. v. FTC, 678 Fed. Appx. 816, 821 (11th Cir. 2016).
26. The FTC might argue, for instance, that while the Third Circuit did not directly address the enforceability concerns animating the Eleventh Circuit's decision, it did hold that Wyndham had received sufficient notice under a "reasonableness" standard that its cyber security practices were deficient. See Data Matters Blog, supra.
27. See ibid.
28. Ibid.
29. See ibid.
30. See ibid.
31. The issue of how cyber security in the healthcare field should be regulated and coordinated has also sparked congressional interest, with bills being introduced on the topic in the past couple of years. See, e.g., HHS Cybersecurity Modernization Act, H.R. 4191 (introduced by Representatives Long (R-MO) and Matsui (D-CA) in October 2017); The Internet of Medical Things Resilience Partnership Act of 2017, H.R. 3985 (introduced by Representatives Trott (R-MI) and Brooks (R-IN) in October 2017); see also, e.g., Letter from Rep. Walden, Rep. Pallone, Sen. Alexander, & Sen. Murray to U.S. Dep't of Health & Human Servs Sec'y Alex Azar, at 2 (June 5, 2018).