The CYBERSECURITY LAW REPORT

www.cslawreport.com Vol. 4, No. 16 June 13, 2018

JUDICIAL DECISIONS

The Devil Is in the Details: *LabMD* Imposes Limitations on the FTC's Enforcement Authority

By Elizabeth McGinn, Sasha Leonhardt, A.J. Dhaliwal, Buckley Sandler LLP

In the latest data security case with significant implications for all enforcement actions, the United States Court of Appeals for the Eleventh Circuit struck down a cease-and-desist order as impermissibly vague. By ruling against the FTC in its long-running and contentious dispute with LabMD, the Eleventh Circuit left unresolved a critical question regarding the scope of the FTC's unfairness jurisdiction, but potentially made a greater impact in imposing due process limitations on expansive, unclear enforcement actions.[1]

The Eleventh Circuit's decision provides a significant setback to the FTC's practice of imposing broad-reaching data security programs upon companies in response to discrete data breaches. The *LabMD* decision not only contains lessons for companies in litigation with regulators, but those involved in negotiating a resolution to an administrative action can also find much to appreciate in the Eleventh Circuit's opinion. Further, the court's decision, though narrow in scope, also provides lessons to all companies holding consumer information on how to protect their data and how best to respond after a data breach.

See also "Lessons and Trends From FTC's 2017 Privacy and Data Security Update: Enforcement Actions (Part One of Two)" (Jan. 31, 2018); Part Two (Feb. 14, 2018).

LabMD Case Background

Factual Background

LabMD was a laboratory that conducted medical tests on patient specimen samples and reported the test results to its physician customers. In 2013, the FTC initiated an administrative enforcement action against LabMD for its alleged failure to employ "reasonable and appropriate" measures to prevent unauthorized access to consumers' personal information.[2]

See also "FTC Data Security Enforcement Year-In-Review: Do We Know What 'Reasonable' Security Is Yet?" (Jan. 25, 2017).

The FTC's complaint arose from two LabMD security incidents. First, a data security firm informed LabMD that it found a LabMD document with consumer information on LimeWire, a peer-to-peer file-sharing program that an employee had installed on a single computer in the accounting department. Although LimeWire was only installed once, it made all of the documents within an entire directory available to anyone using LimeWire. One of these documents was an internal LabMD report containing names, Social Security numbers, dates of birth, insurance information, and medical records of approximately 9,300 LabMD patients. The data security firm informed LabMD of the breach, and LabMD removed LimeWire and prevented any further sharing of the report. The data security firm then provided the report to the FTC, but despite a multi-year investigation the FTC never identified any evidence of identity theft or misuse of any consumer information. Further, all of the evidence in the subsequent litigation indicates that, besides the data security firm, no one else ever downloaded or even viewed the report while it was available on LimeWire.

During the second incident, law enforcement found documents associated with LabMD while searching a house as part of an unrelated investigation into utility bill fraud. The documents contained names and Social Security numbers of approximately 600 consumers from LabMD's billing software. As above, even though these documents were removed from LabMD, there is no evidence of identity theft or misuse of the documents or information.

ALJ Decision

At the initial trial before the FTC's Administrative Law Judge (ALJ), the ALJ held that the FTC failed to show that LabMD's "failure to employ reasonable data security constitutes an unfair trade practice."[3] For an act or practice to be "unfair," it must meet three critical elements: (i) the act or practice causes or is likely to cause substantial injury to consumers; (ii) which is not reasonably avoidable by consumers themselves; and (iii) which is not outweighed by countervailing benefits to consumers or to competition.[4]

The ALJ held that LabMD's data breach was not "likely to cause substantial injury to consumers."[5] Regarding the first incident, the ALJ found insufficient evidence to conclude that

the limited exposure of the internal report resulted in any substantial harm. The ALJ specifically noted that because the LabMD report was only downloaded by the data security firm and LabMD had taken steps to make additional downloads impossible, there was no "likelihood of harm" under the FTC Act.[6]

Regarding the second incident, the ALJ held that there was an insufficient causal connection between the documents and LabMD's failure to reasonably safeguard information contained in its electronic files. The ALJ concluded that the agency failed to show any proof of actual consumer injury and rejected the theory that a hypothetical risk of future harm met the requirements of Section 5. The ALJ concluded that, "[t]o impose liability for unfair conduct under Section 5(a) of the FTC Act, where there is no proof of actual injury to any consumer, based only on an unspecified and theoretical 'risk' of a future data breach and identity theft, would require unacceptable speculation and would vitiate the statutory requirements of 'likely' substantial consumer injury."[7]

Commission Decision

The FTC staff promptly appealed to the full Commission, which reversed the ALJ and held that the LabMD data breach was "unfair" to consumers.[8] The Commission held that "the ALJ applied the wrong legal standard for unfairness" and that the correct inquiry was whether a data breach posed a "significant risk" of injury to consumers at the time it occurred. The Commission also noted 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."[9] Emphasizing its responsibility to prevent future harm, the Commission stated that it "need not wait for consumers to suffer known harm at the hands of identity thieves" before initiating enforcement proceedings. [10]

See also "Takeaways From the FTC's Revival of the LabMD Action " (Aug. 24, 2016).

LabMD Eleventh Circuit Decision

LabMD appealed the Commission's decision to the Eleventh Circuit last year. The briefs filed by both LabMD and the FTC focused almost entirely on a novel question regarding the FTC's data breach enforcement powers: if no consumers were harmed by – and there is no risk of future harm from – a data breach, was the data breach "unfair"? Section 5 of the FTC Act defines an "unfair" act or practice as one that "causes or is likely to cause substantial harm to consumers."[11] Based upon the briefing and unique factual situation in this case, many had hoped that the court would similarly answer this critical question regarding the scope of unfairness under the FTC Act.

In its June 6, 2018, opinion, the court noted that unfairness is not an abstract concept, but rather the question of whether an individual act or practice that is unfair must be "grounded in statute, the common law, or the Constitution." The court then stated that the apparent source of unfairness in the FTC's complaint was the common law of negligence – specifically, "that LabMD's negligent failure to design and maintain a reasonable data-security program invaded consumers' right of privacy and thus constituted an unfair act or practice." [12] However, rather than applying this unfairness standard to LabMD's actions and providing some much-needed clarity to the law, the court assumed "arguendo [for purpose of argument] that the Commission is correct" in finding that LabMD had committed an unfair act or practice and instead chose to resolve this case on a different basis.

Instead, the Eleventh Circuit resolved this case entirely based upon an argument that the combined briefs of both LabMD and the FTC spent only six pages addressing: whether the Commission's cease-and-desist order was impermissibly vague and therefore unenforceable. The order issued by the Commission required the company to "establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of [consumers'] personal information." Critically, the order gave no further guidance as to what a "reasonably designed" program would entail.

The Eleventh Circuit held that this cease-and-desist order "does not enjoin a specific act or practice"[13] and therefore was unenforceable. Because LabMD could not reasonably determine in advance what actions and practices would violate this order, the Commission had effectively denied LabMD due process. Further, because the FTC can enforce its cease-and-desist order in federal district court – and impose significant fines against LabMD – the order could not stand. In the court's view, upholding such an order would make it "as if the Commission was LabMD's chief executive officer and the court was its operating officer." Accordingly, the Eleventh Circuit vacated the Commission's cease-and-desist order in its entirety.

The CYBERSECURITY LAW REPORT

www.cslawreport.com Vol. 4, No. 16 June 13, 2018

Lessons Learned From LabMD

LabMD provides a number of lessons that companies may want to consider about how to protect against – and respond to – a data breach:

- Limit access to sensitive data to only those who have a demonstrated business need for access. In many instances, the weakest parts of a data security program are the individual users – as was the case in *LabMD*, where a single employee's actions exposed the company to significant legal risk. Limit this exposure by limiting the number of individuals with access to critical data, and require separate user accounts to limit access on a user-by-user basis.
- Limit administrator privileges on computers to prevent installation of unauthorized file-sharing programs. Administrative access, which allows users to install new programs on individual computers, can lead to vulnerabilities in an otherwise-secure network. Even if individual employees are trustworthy, the addition of unknown programs (such as the file-sharing program in *LabMD*) can provide third parties with access to a closed network. Administrator privileges should be limited to individuals in the IT department, approved by appropriate management, and governed by robust policies and procedures.
- Ban access to high-risk IP addresses, such as those used by file-sharing websites and third-party email services. For many companies, there is no business purpose for employees to access these websites, yet they can pose a real risk to data security. If your business requires using such websites, limit access only to those employees with a demonstrated need to access these websites and only provide limited, temporary access.
- Create and monitor firewalls to identify prohibited data activity. New file-sharing websites emerge every day. When designing your network, consider using firewalls to limit and monitor access between computers on your network and between your computers and the internet. By tracking the type and volume of user activity with a robust firewall, companies can identify data-traffic patterns that may suggest unauthorized access to internal networks.
- Train – and re-train – all employees (including administrative employees who do not typically handle consumer data) on data security requirements. Data security threats are constantly evolving, and continued training of employees is critical to keep up with these threats. Otherwise well-intentioned employees may not realize that their actions create systematic data vulnerabilities for a company, and further educating these employees can prevent problems before they start. Ongoing security awareness training is particularly important because it helps create a corporate culture of awareness.
- When notified of a data breach, immediately take steps to prevent further sharing of unauthorized material. It is vital to identify a compromised system as soon as possible and fix the data leak to prevent future attacks. While this can be handled either in-house or by a third party, it is critical to stop further sharing – both to protect consumer data and to limit the scope of the company's legal liability.
- Comply with all federal and state data breach laws. Several states have recently passed new or updated existing laws requiring companies to disclose a data breach to affected consumers. Be sure you know where your consumers are located and which laws apply.

See also "Analyzing New and Amended State Breach Notification Laws" (Jun. 6, 2018).

Further, if a data breach ever reaches the point of an enforcement action, companies can take several cues from the recent Eleventh Circuit's decision.

- Determine whether the alleged practice is truly "unfair." The *LabMD* opinion states that an allegedly unfair act or practice be "grounded in" statutory law, common law, or the Constitution. Critically, however, the Eleventh Circuit never defined what "grounded in" means: how similar must an act or practice be to a violation of an existing law to be "unfair"? If an act or practice complies with existing law, would the Eleventh Circuit hold that such act or practice cannot be unfair? Further, the *LabMD* court declined to actually rule on whether an act or practice that did not harm consumers in the past and could not harm consumers in the future is unfair. Companies facing allegations of unfairness should look to the *LabMD* decision for guidance on the unfairness standards that may apply to a data breach claim.

- Evaluate whether proposed injunctive remedies are unfairly vague. The court also emphasized that a cease-and-desist order under the FTC Act must be clear enough that the recipient of the order has fair notice of what actions are prohibited. While the *LabMD* ruling provides an important limitation on the FTC's ability to enter into data privacy cease-and-desist orders in the future, this ruling may be more broadly applicable to other companies facing demands for injunctive relief from federal regulators. Such demands are a standard part of settlement agreements with the Commission and other regulators, and the Eleventh Circuit's decision makes clear that such injunctive demands must be clear, specific, and enforceable.

- Ensure that any proposed remedy is tailored to the alleged harm. The Eleventh Circuit was critical of how the FTC used a single specific data breach as an "entry point" to enter a sweeping cease-and-desist order that touched every aspect of LabMD's data security practice. Companies facing future enforcement actions can turn to the *LabMD* decision to limit the scope of any injunctive relief to focus only on the source of any alleged harm.

Although the *LabMD* court did not answer whether a data breach that did not cause any financial consumer harm was unfair, its opinion nevertheless provides helpful guidance on the breadth and scope of the Commission's ability to impose injunctive relief. By setting pragmatic limits on such injunctive relief, the Eleventh Circuit helped to generate certainty in the wake of an enforcement order.

Elizabeth McGinn, a partner at Buckley Sandler, helps clients to identify, evaluate and manage risks associated with cybersecurity, internal privacy and information security practices, as well as those of third-party vendors. She advises clients during regulatory investigations and enforcement matters by state and federal agencies, including the CFPB, FTC, DOJ, NYDFS and state attorneys general. In addition, she works closely with companies on proactive cybersecurity readiness, including developing policies and procedures, handling investigations of data security and privacy violations and counseling clients on data collection and sharing issues.

Sasha Leonhardt, counsel, represents financial services and technology companies in a wide range of enforcement, litigation, and regulatory matters. He helps clients in resolving government investigations and enforcement actions before a variety of federal and state agencies, including the DOJ, CFPB, OCC, and state attorneys general. He also assists companies with internal investigations and counsels companies on legal compliance and best practices regarding data privacy issues.

A.J. Dhaliwal counsels clients in the financial services industry, primarily in government enforcement, regulatory and compliance matters. He has experience handling complex civil litigation and internal investigations involving banks and non-banks in CFPB, DOJ, and FDIC actions alleging violations of consumer protection laws. In addition, he counsels directors with respect to regulatory proceedings and litigation involving troubled and failed financial institutions, as well as non-bank servicers in consumer protection investigations and enforcement actions brought by state attorneys general.

[1] In the Matter of *LabMD, Inc.*, No. 9357, 2016 WL 4128215 (F.T.C. July 28, 2016), vacated, *LabMD, Inc*. v. Fed. Trade. Comm., No. 16-16270 (11th Cir. Jun. 6, 2018).
[2] In re *LabMD Inc.*, No. 9357, 2015 WL 7575033, at *2 (F.T.C. Nov. 13, 2015).
[3] Id. at *9.
[4] See 15 U.S.C. § 45(n).
[5] In re *LabMD Inc.* at *9.
[6] Id.
[7] Id.
[8] In the Matter of *LabMD, Inc.*, No. 9357, 2016 WL 4128215, at *1 (F.T.C. July 28, 2016). For purposes of clarity, this article uses the term "Commission" solely to refer to the leadership of the FTC sitting as an adjudicative body, and the term "FTC" to refer to the enforcement and policy arms of the FTC.
[9] Id. at *17.
[10] Id. at *20.
[11] 15 U.S.C. § 45(n) (2012).
[12] *LabMD, Inc.* v. Fed. Trade. Comm. at 17-18.
[13] *LabMD, Inc.* v. Fed. Trade. Comm. at 30.