Crowell

Client Alert

Eleventh Circuit Reins in the Federal Trade Commission

June 12, 2018

The long-running legal battle between the Federal Trade Commission and LabMD, the now-shuttered medical laboratory it accused of having unfairly lax data security practices, has resulted in a milestone decision from The Eleventh Circuit. The Eleventh Circuit has ruled in LabMD's favor regarding the scope of the FTC order at issue, and its decision not only weakens the FTC's ability to issue broad cease and desist letters in the cybersecurity space, it may also have wide-reaching impacts on all of the FTC's consumer protection orders.

LabMD operated as a laboratory that collected patient data and specimens to perform diagnostic tests for cancer. While the lab is now defunct, LabMD still exists as a company and maintains patient data in its computer systems. In 2005 a billing manager at LabMD downloaded a peer-to-peer file sharing app called LimeWire onto her work computer in violation of company policy. Tiversa Holding Corp, which specializes in data security, used the file sharing program LimeWire to access the billing manager's computer and download a nearly 2,000 page file containing the PII of 9,300 companies. After LabMD declined several offers by Tiversa to improve their system security, Tiversa informed the FTC of the breach.

The FTC brought a Section 5(a) complaint against LabMD alleging that the company's failure to secure patient data constituted "unfair acts or practices" within the meaning of Section 5. The FTC filed its complaint as an administrative action before the Commission, rather than proceeding in federal court. The dispute wound its way through the FTC administrative process over several years, ultimately resulting in the full FTC determining that LabMD "failed to implement reasonable security measures to protect the sensitive consumer information on its computer network," essentially concluding that the Lab's entire data security operation was an unfair act or practice. The FTC then issued a cease and desist order against LabMD that required LabMD to implement and maintain a data security system "reasonably designed" to the FTC's satisfaction. LabMD appealed the order to the Eleventh Circuit.

On appeal, the Court assumed *arguendo* that the Commission correctly determined that LabMD's data protection protocols were negligently designed and implemented. However, it ruled the FTC's cease and desist order could not be enforced due to vagueness and lack of specificity. Agreeing with LabMD, the Court found that this lack of specificity amounted to a denial of due process as the order did not appropriately give the defendant notice of what data security requirements would be required. For example, the order required LabMD to overhaul its data-security program "to meet an indeterminable standard of reasonableness." The Court stressed the uncertainty that would arise if the FTC in the future sought to enforce such a vague order by contempt proceeding in court, as what would constitute "reasonable" security measures might be an ever-shifting and debatable issue, depending on when the case was brought and what the state of the industry was at that time.

The Eleventh Circuit offered an example of what Commission enforcement of the order might entail. Hypothetically, if LabMD implemented improved data security measures, but the FTC found the results fell short of its undefined standard of "reasonableness," the two parties would end up before a district court with equally qualified experts arguing over the reasonableness of the steps taken to conform with the order. As a result, the district court would have no choice but to conclude that the Commission did not and could not prove by clear and convincing evidence that LabMD violated the cease and desist order. The Commission would then have to move to *amend* the order to provide greater specificity. The result would be the district court micromanaging the process of compliance. This scenario, the Eleventh Circuit concluded, "is a scheme Congress could not have envisioned."

The decision signals that at least one influential court has questioned FTC orders containing vague "reasonable" data protection standards. This decision will certainly be brought up in other proceedings by defendants facing similar data security proceedings. However, the decision's influence will not likely end there. Numerous FTC orders, including those in areas outside of data security, contain forward-looking compliance obligations that are based on standards of "reasonableness." For example, the FTC's Policy on Advertising Substantiation is founded on the principle that advertisers must possess a "reasonable basis" for advertising claims. What constitutes a "reasonable basis" can shift over the course of 20 years. Indeed, the FTC has struggled in contempt proceedings to define "reasonable" substantiation with precision such that it can satisfy its burden of providing "clear and convincing" proof that a defendant violated an "unambiguous" requirement of the order. *See, e.g., United States v. Bayer*, D.N.J. No. 07-01 (DLL) (2017); FTC v. Lane Labs-USA, 624 F.3d 575 (3d Cir. 2010). As the court stated in *Bayer*, "specificity in the terms of consent decrees is a predicate to a finding of contempt, because [a defendant] will not be held in contempt . . . unless the order has given [it] fair warning."

There are three key takeaways from these developments.

First, the decision may push the FTC to propose far more specific technological and operational measures that a company must implement pursuant to future data security orders. However, there is a tension between imposing such a requirement and the FTC's typical order term of 20 years. Perhaps the FTC may have to consider imposing shorter-duration orders, or, alternatively, sunsetting-order provisions dealing with specific technological mandates after a few years, while keeping in force reporting obligations for longer periods.

Second, the ruling picks at a wound that the FTC has been trying to conceal since the *Lane Labs* and *Bayer* decisions; that is, how best to bring enforcement regarding the whole universe of existing orders that are arguably vague with respect to substantiation requirements. Rarely is there unanimity among experts regarding how many tests, and what kinds of tests, are required for claims support. The latest *LabMD* decision adds to precedent that casts some doubt on the FTC's ability to bring contempt proceedings regarding such orders. At minimum, it may embolden more defendants to fight the FTC in court.

Third, the ruling might provide an opportunity for companies currently subject to FTC orders to request that the FTC modify its order to create greater specificity and certainty for both the company and the FTC. The *LabMD* court all but signaled that defendants perplexed by what is required of them might consider approaching the

FTC to negotiate a more concrete set of requirements. This would remove doubt and provide a clearer set of compliance obligations that could provide a sort of “safe harbor” for compliance.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Jeffrey L. Poston
Partner – Washington, D.C.
Phone: +1.202.624.2775
Email: jposton@crowell.com