New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 260—NO. 25
MONDAY, AUGUST 6, 2018

Outside Counsel

Expert Analysis

11th Circuit Decision in LabMD Case Could Have Repercussions Beyond the FTC

On June 6, the United States Court of Appeals for the 11th Circuit issued a long-awaited decision in *LabMD, Inc. v. FTC*. The case had an extensive history already, dating back to a 2008 data leak that had exposed patient information for several thousand individuals through the now defunct file-sharing service, LimeWire. The FTC investigated the leak, ultimately finding that *LabMD* had failed to undertake reasonable efforts to protect patient information from disclosure. Instead of settling, as more than 60 companies have done since the FTC began enforcement efforts in relation to data privacy in 1999, LabMD did the unthinkable. It challenged the FTC's findings as well as its authority to enforce in the cyber security arena, ultimately taking the matter to the 11th Circuit for review.

In its decision, the 11th Circuit had the opportunity to address several key and contested issues in relation to the FTC's enforcement efforts: Does the FTC have authority under the FTC Act to enforce in this arena in the first place; does the FTC have plenary authority to enforce in relation to data breaches also covered under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and was the FTC simply wrong in its findings that *LabMD* had violated the FTC Act by not instituting controls that would have avoided the LimeWire-enabled data leak? The court, however, focused instead on the cease and desist order issued by the FTC, requiring *LabMD* to implement a comprehensive information security program "reasonably designed to protect the security, confidentiality and integrity of personal information collected from or about consumers."

By **Paul Greene**

And **Daniel J. Altieri**

Analyzing the order's specific requirements, the 11th Circuit found it fatally lacking in detail, noting that the order effectively left it up to the District Court to determine whether *LabMD*'s activities to secure patient data for the next 20 years were "reasonable." Applying bedrock law concerning the enforceability of injunctive orders, the 11th Circuit concluded that the lack of detail in the *LabMD* order made it unenforceable, leaving for another day the issues of whether the FTC had overstepped its bounds in relation to the order as well as the other challenges brought by *LabMD* in the underlying case.

The decision has called into question a cornerstone of FTC enforcement in relation to cyber security: its ability to remain flexible to address data incidents that are inherently fact specific, many of which deal with security threats and failings not previously anticipated. This kind of flexibility has been upheld previously, specifically in *FTC v. Wyndham Worldwide Corp*., where the Third Circuit upheld a District of New Jersey holding that the FTC has authority under Section 5(a) of the FTC Act to enforce against allegedly "unfair" and "deceptive" business practices in relation to cyber security. It must be remembered in this regard that the FTC has no regulations guiding its cyber-enforcement efforts, relying only on the language of the FTC Act, promulgated originally in 1914 and amended in 1938, generally declaring "unfair" and "deceptive" business practices to be unlawful. *See* 15 U.S.C. § 45(a).

> The 11th Circuit found the order fatally lacking in detail, noting that it effectively left it up to the District Court to determine whether LabMD's activities to secure patient data for the next 20 years were "reasonable."

Although the flexibility upheld by the Third Circuit remains in place after the *LabMD* decision, it has been significantly curtailed, with possible ripple effects to be felt by administrative agencies and authorities beyond the FTC. This is because, alongside the

PAUL GREENE, *a partner, and Daniel J. Altieri, a senior associate, are members of the Privacy and Data Security practice group at Harter Secrest & Emery.*

FTC's nearly two-decade-long efforts to enforce in the data privacy and security space, a patchwork of overlapping state-law and regulatory requirements has sprung up, and certain of these requirements may feel the impact of the 11th Circuit's decision.

State Unfair and Deceptive Acts Mirror FTC Act

To begin with, all 50 states and the District of Columbia have Unfair and Deceptive Acts and Practices ("UDAP") acts. Many of these UDAP acts mirror Section 5(a) of the FTC Act closely, and state attorneys general have been using UDAP acts to enforce in the cyber security space for years. Case in point: New York, under its data breach notification statute, N.Y. Gen Bus. Law § 899-aa, can issue fines for failure to provide notice to New York residents in relation to a data breach. Section 899-aa, however, is not as flexible as New York's UDAP statute, N.Y. Gen. Bus. Law § 349, allowing for fines only in cases involving "knowing" or "reckless" violations of § 899-aa, with a maximum fine per occurrence of $150,000.

It is no surprise, then, that states often turn to their UDAP authority to enforce in relation to data breaches. They also do this across state lines, coordinating their efforts in relation to multi-state data breaches, where state-law UDAP requirements are often more harmonized than data breach notification requirements and fines. Case in point: the August 2017 settlement between Nationwide Mutual Insurance Company and 33 state attorneys general and administrative agencies (including the attorney general of the District of Columbia), resulting in a $5,500,000 fine paid by Nationwide, as well as Nationwide's agreement to engage in three years of monitored patch management, together with monitoring of and scanning for "Common Vulnerabilities and Exposures" ("CVEs") affecting Nationwide's systems and the software it uses.

The Nationwide Assurance of Voluntary Compliance ("AOVC"), which is the state-law analog of the consent order used by the FTC in relation to FTC Act enforcement, goes both further than and not as far as the *LabMD* order struck down by the 11th Circuit. In doing so, it may become an example for future UDAP enforcement on the state-law level post-*LabMD*. To begin with, the Nationwide AOVC is far shorter in duration than the standard FTC order, which lasts for 20 years and is binding on successors and assigns of the settling party. Although not directly discussed in the 11th Circuit's decision, the extreme length of the FTC form order could have added to the 11th Circuit's reticence to leave an affected company's obligations in relation to "reasonable" cyber security efforts so open-ended for so long. In this regard, the Nationwide AOVC, and any state-law UDAP order that follows its structure, may avoid harsher scrutiny by limiting its temporal scope.

The Nationwide AOVC exceeds the FTC's *LabMD* order in the detail it provides concerning monitoring and addressing security concerns. Instead of requiring "reasonable safeguards to control the risks identified through [an FTC-ordered] risk assessment," as contained in the *LabMD* order, the Nationwide AOVC focuses specifically on patch management and specific CVEs, which represent a collaboratively established list of over 100,000 security vulnerabilities identified by over 88 CVE Numbering Authorities ("CNAs") from around the world. This focus on specific CVEs, as updated from time to time by participating CNAs, provides both the flexibility sought by the FTC in its form cease and desist order, and the detail found lacking in that order by the 11th Circuit. Importantly, however, this focus also cedes the authority to define compliance criteria to a non-governmental entity, which may be anathema to an administrative agency's efforts to seek broad enforcement authority.

Such a lack of ultimate control may be key in a post-*LabMD* regulatory landscape. Indeed, other regulatory schemes in the privacy and data security space have long ceded a certain level of control to regulated entities themselves, allowing such entities to tailor a comprehensive information security program to their own needs and circumstances, based upon an internal risk assessment. These include HIPAA, the Gramm-Leach-Bliley Act and state analogs such as 201 CMR 17.00 in Massachusetts, and the New York State Department of Financial Services cybersecurity regulations, 23 N.Y.C.R.R. Part 500, which incorporates a risk assessment requirement as of March 1, 2018.

Yet flexibility on the front end in relation to an information security program does not always mean effectiveness on the back end when it comes to enforcement, as shown in the *LabMD* order, which also bases its requirements on an internal risk assessment. This will especially be the case in New York if the recently proposed SHIELD Act is passed, which would add a new § 899-bb to the General Business Law to require "any person or business that owns or licenses computerized data which includes private information of a resident of New York" to develop and implement "reasonable safeguards to protect the security, confidentiality and integrity of the private information including, but not limited to, disposal of data." Although the New York State Legislature, through which the SHIELD Act has been advancing, likely has the authority to set such open-ended standards, any order issued under the SHIELD Act, or any state-law UDAP order merely mouthing a "reasonableness" standard, is likely insufficient and unenforceable post-*LabMD*.

In this regard, the 11th Circuit's decision striking the FTC's final *LabMD* order will likely be felt far outside of the realm of FTC enforcement. Although there is little consensus as to what constitutes "reasonable" cybersecurity practices in every circumstance, reference to consensus-based risk-registers such as CVEs or even governmentally created approaches to security such as the National Institute of Standards and Technology's Cyber Security Framework, may become more of the norm, as the FTC and attorneys general seek to enforce against what they see as unfair and deceptive, or at least unreasonable, cybersecurity practices.