

What To Watch As LabMD, FTC Square Off Over Data Security

By **Allison Grande**

Law360, New York (June 20, 2017, 10:49 PM EDT) -- LabMD and the Federal Trade Commission are set to go before the Eleventh Circuit on Wednesday in a pivotal case that will have a sweeping impact on the commission's ability to regulate corporate data security.

The yearslong battle reached the court last year, shortly after the heads of the FTC released an opinion in July 2016 that overturned their own administrative law judge. In that decision, the commissioners concluded that the lab's failure to employ "basic" security precautions led to an unauthorized disclosure of sensitive medical data that caused "substantial" harm to consumers in violation of the unfairness prong of Section 5 of the FTC Act.

"This case is a consequential test of the Federal Trade Commission's authority as a data security regulator," said Craig A. Newman, a partner with Patterson Belknap Webb & Tyler LLP and head of its privacy and data security practice. "The Eleventh Circuit appeal will have far-reaching implications for organizations under the FTC's watch, however it is decided."

If the appellate panel comes down in favor of the FTC and concludes that LabMD's security practices were unreasonable, the commission will not have to show proof of actual consumer harm or injury to mount data security enforcement actions under Section 5. That means the more than 60 data security consent decrees the agency has penned over the past two decades "will be viewed as instructive precedents indicating what data security practices the FTC deems 'unfair,'" Newman said.

But if, on the other hand, the Eleventh Circuit agrees with LabMD that concrete consumer harm is required to bring an enforcement action under Section 5's unfairness prong, "the enforcement bar will be raised — requiring the FTC to show more than just speculative injury — which will likely toughen an organization's stance if the FTC comes knocking," Newman said.

Here, court watchers lay odds on what issues are likely to dominate the arguments, and what clues to look for in trying to decode how the appellate panel might rule.

Dueling Harm Arguments

Those who have followed the case closely since its inception in 2013 expect the bulk of Wednesday's 30-minute oral argument session in Miami to focus on the issue that has been at the core of the dispute for some time: whether the language of Section 5 requires the FTC to demonstrate actual concrete harm

similar to what private plaintiffs must show to establish Article III standing, or whether a more speculative injury is enough.

“If the court seems interested in restricting the FTC’s activities to situations that involve only some higher level of consumer harm, that will have a material impact on FTC activity in general,” said Wiley Rein LLP privacy practice chair Kirk Nahra. Nahra noted that such a determination would put the commission in a similar position to plaintiffs when it comes to harm, while setting the agency apart from other privacy regulators that don’t need to show consumer harm if they find a violation.

Under the unfairness prong of Section 5, the commission is required to show that an unlawful practice “causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.”

The FTC has interpreted this language to mean that it does not need to wait for consumers’ data to be misused in order to act. But LabMD has countered that the commission went too far in concluding that the purported leak of a file containing data on nearly 10,000 patients who never complained of any harm constituted the type of “substantial” injury to support a Section 5 claim. Attorneys expect both parties to continue to vigorously press these arguments Wednesday.

On the FTC side, the commission is likely to focus on its important role in protecting consumers from a broad range of harms that have both already materialized and are highly likely to come to fruition, and may even raise the point that “without such prescriptive powers, the U.S. will be found to not comply with various cross-continental data transfer pacts and regulations,” according to Troutman Sanders LLP partner Mark C. Mao.

Across the table, LabMD is likely to home in on the leaked patient data file that formed the basis for the FTC’s claims. The lab alleges the file was stolen from its servers by cybersecurity firm Tiversa in retaliation for the lab not purchasing its services, and it says no other party ever had access to the data.

“If the evidence presented to the FTC later proves to be specious and questionable, it is reasonable to question whether or not the FTC really has authority to act against ‘unfair and deceptive’ conduct, especially ex post facto,” Mao said.

The lab is also likely to attack the FTC commissioners for concluding in their July opinion that there was a substantial likelihood of harm because there was a high “magnitude” of potential harm to the 9,300 consumers whose data was exposed, concepts that Mao noted are “not the same thing.”

“Just because I can win hundreds of millions in a state lottery does not mean that there is a substantial likelihood of me winning the lottery,” Mao said. “Look for LabMD to destroy that argument.”

LabMD CEO Mike Daugherty indicated Tuesday that this line of questioning was one that his side was keen on pursuing during oral arguments.

“Now we’re down to a semantic debate over whether the FTC can get away with twisting the English language by stating in court, with a straight face, that likely equals unlikely,” Daugherty told Law360.

Impact of New Leadership at FTC

While the FTC’s arguments surrounding harm have remained consistent throughout the course of the

long-running legal dispute, attorneys noted that since the FTC commissioners handed down their ruling last July, the commission has gone from being led by Democrat Edith Ramirez to Republican Maureen Ohlhausen. Ohlhausen has repeatedly stated since taking over in February that she intends to shift the agency's focus away from speculative harms and instead devote the agency's resources to cases in which business activity has led to actual and substantial harm.

Attorneys who are planning to tune into the oral arguments Wednesday wonder whether the new acting chair's stance on the harm issue will impact how the FTC presents its case before the Eleventh Circuit panel.

"The LabMD argument will provide an important window into how the new FTC will deal with the all-important question of 'harm' in the context of data security enforcement actions," Covington & Burling LLP data privacy and cybersecurity chair Kurt Wimmer said. "The argument presents an opportunity for the FTC to explain its current view of 'harm,' and how it should be applied in the LabMD case."

Kilpatrick Townsend & Stockton LLP cybersecurity, privacy and data governance practice co-leader Jon Neiditz pointed out that in light of the shifting view of harm at the top of the agency, "a ruling against the FTC could in fact serve acting Chairman Ohlhausen's express goal of trying to refocus the FTC on harm as the basis for enforcement."

"Ohlhausen's speeches and dissents have reflected a balance sorely missing on both the left and the right, a balance rooted in what she herself has called 'humility,'" Neiditz said. "My hope — even though the voices on left and right are more arrogant and strident than ever before — is that LabMD can return the FTC to focus on cases in which consumers are in fact likely to suffer unjustifiable harm."

Back-Burner Issues

While the circuit judges' reaction to the harm argument will be the primary factor to watch, attorneys say the long and strange history of the dispute gives the panel the ammunition to throw some curveballs at the parties that could lead to surprising results.

"This is unlike any other data security enforcement action we've seen in the past 20 years," Newman said. "It's got all these cloaks and daggers, including allegations of government overreach, evidence tampering and a witness getting immunity. This is not the stuff of a typical data security enforcement action."

Besides arguing that the commission hadn't met its burden to show that consumers had been harmed, LabMD has also contended during the course of litigation that Section 5 does not permit the FTC to ever characterize lax data security practices as "unfair," even if the commission can prove consumer harm.

That argument formed the basis of the first-ever challenge to the agency's data security enforcement authority, mounted by Wyndham Worldwide Corp. That dispute made its way to the Third Circuit, which ruled in August 2015 that the FTC does have the power to regulate corporate data security.

"If the court is at all sympathetic to LabMD on this issue, that would be enormous — that's the premise of all of the FTC's data security cases," Nagra said. "That would create the possibility of a huge gap in security enforcement, and in theory could push Congress to actually act in this area."

LabMD in its briefs has also made the argument that even if the FTC does have the authority to police

data security, it chose poorly in pressing a case against the lab. To support this point, the lab has contended that the commission's claims were already covered by and ultimately trumped by the Health Insurance Portability and Accountability Act, and that the commission had only decided to go after the LabMD in retaliation for Daugherty publishing a book, "The Devil Inside the Beltway," that sharply criticized the agency for its aggressive pursuit of the lab.

Daugherty has continued to denounce the FTC, as he did when speaking with Law360 on Tuesday.

"The big picture of the LabMD case shows how much power and money the FTC squandered to drag LabMD through so much litigation on such flimsy evidence," Daugherty said. "The FTC lied nonstop and was caught red-handed ... and yet that still didn't stop them."

Daugherty, who was forced to shutter his lab in 2014 due to the expense of fighting the FTC, continued, "There was never a victim, never a spread of data, and never any harm from Tiversa breaking in, taking our file, keeping it for extortion and giving it to the government. That file went nowhere else and the FTC knows it, but best throw out red herrings by attacking medical professionals and patients rather than have the light shine back on the FTC's corruption and incompetence."

The FTC did not respond to a request for comment on this story, but the commissioners did indirectly respond to some of Daugherty's criticisms in their July opinion, saying that while they found Tiversa's CEO not to be credible or reliable, "there is no evidence that Tiversa acted as an 'agent' or 'adjunct' to the FTC in obtaining the [patient data] file, much less that anyone at the FTC 'exercised coercive power' compelling Tiversa to do so."

While these back-burner issues have largely fallen by the wayside, they could still be picked up by the appellate panel — and if they are, could lead to a much narrower outcome, attorneys say.

"This has always been a weird case — the security problems that were identified, while clearly not good, may not have been anywhere near as bad as many other cases," Nahra said. "So the narrowest reading of this case — which is possible — would be that the FTC made a mistake on the facts of this case, without the court getting into any broader philosophical discussion."

LabMD is represented by Doug Meal, David Cohen, Michelle Visser and Douglas Hallward-Driemeier of Ropes & Gray LLP.

The FTC is represented by staff attorneys Joel Marcus, Theodore Metzler and Michael Hoffman.

The case is LabMD Inc. v. Federal Trade Commission, case number 16-16270, in the U.S. Court of Appeals for the Eleventh Circuit.

--Editing by Mark Lebetkin and Philip Shea.