Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

FTC's Data Security Authority Limited In LabMD Ruling

By **Allison Grande**

Law360, New York (November 17, 2015, 10:58 PM ET) -- In tossing the Federal Trade Commission's data security suit against LabMD, an administrative law judge set a high bar for the agency to prove consumer harm similar to the one that has consistently plagued plaintiffs in private litigation over data breaches, attorneys say.

Chief Administrative Law Judge D. Michael Chappell brought to a close a lengthy administrative proceeding by releasing a highly anticipated initial decision late Friday. The decision rejected the commission's argument that LabMD Inc.'s purported failure to institute reasonable and appropriate data security standards constituted an unfair trade practice under Section 5 of the FTC Act because the conduct caused or is likely to cause substantial injury to consumers.

Offering one of the first judicial assessments of how Section 5 applies in a data security context, the judge's 92-page decision endorsed a narrow view of the "harm" required by the statute in concluding that hypothetical or theoretical harm caused by the lab's conduct was insufficient to maintain the commission's allegations.

"The reason that the decision was so shocking and important is that because the security standard imposed by the FTC has never been challenged in any court, the FTC has created an enormous castle of air in recent years that everyone has come to believe in," Kilpatrick Townsend & Stockton LLP big data, privacy and information security practice co-leader Jon Neiditz told Law360. "But with this decision, that whole castle of air has been completely deflated."

By requiring a showing of probable and not just possible consumer injury in order for the FTC to sustain a data security claim under Section 5, the administrative law judge's decision moves the commission's pleading burden closer to that required by private plaintiffs in class action litigation over data breaches, attorneys noted.

"This is a very important decision because it essentially equates the FTC's enforcement requirements with the same kinds of standards that private litigants must meet in connection with data breach cases," Wiley Rein LLP privacy practice chairman Kirk Nahra said. "This decision makes it much tougher for the FTC to act."

In private litigation, plaintiffs in class actions over data breaches impacting eBay Inc., P.F. Chang's China Bistro Inc. and a range of other businesses have been stymied by the requirement that they must show actual or imminent harm in order establish Article III standing.

Before the administrative judge's ruling Friday, the FTC had established a body of consent decrees — 53 of the 55 data security cases that the regulator has brought during the past decade have been settled — that are based solely on the commission's assertion that the security failings of the accused business were sufficient to establish the "substantial injury" required by Section 5.

The approach allowed the commission to operate like a regulator such as the U.S. Department of Health and Human Services' Office for Civil Rights, which is not required to show harm because the Health Insurance Portability and Accountability Act permits the department to pursue covered entities and their business associates for mere statutory violations.

However, Section 5 mandates a different approach — namely that the commission needs to show that an act or practice caused 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 competition" — a standard driven home by the administrative law judge's ruling.

"It's established a higher bar for harm than anybody, including the FTC, imagined," Neiditz said. "The FTC has believed that it has complete latitude to bring actions in the absence of any probability of harm, but this decision shows that they have to establish the probability of harm."

The decision marks the second time a court has tackled the issue of the scope of the commission's Section 5 authority when it comes to data security cases.

The first significant ruling in this area came in August, when the Third Circuit addressed the broader question of whether Section 5 permits the commission to regulate the data security practices of private companies such as Wyndham Worldwide Corp. — a question that it resolved in favor of the FTC.

"After the Wyndham decision, the general feeling was that private litigants would continue to have an uphill battle, while the FTC would have an easier time bringing actions," Foley Hoag LLP litigator Christopher Hart said. "What the LabMD decision suggests is that this might not be the case, and that FTC discretion is not unfettered and it needs to be able to show something more, dependent on the facts of the case."

While the LabMD case is likely far from over — if the FTC decides to challenge the decision, it would be reviewed by the commissioners, and could then be further appealed to the courts — the administrative law judge's detailed opinion is poised to have an immediate impact on the regulator's aggressive data enforcement agenda, attorneys said.

"The case delivers a warning that the FTC is going to be held to what the statute requires, which is basically what the administrative law judge said, that the commission utterly failed to carry its burden under Section 5 to ensure that it was likely that consumers suffered a substantial injury," said Craig A. Newman, a partner with Patterson Belknap Webb & Tyler LLP and chairman of the firm's privacy and data security practice.

The decision is likely to make the commission more selective about not only the cases it brings, but the sources it uses, given that it was criticized for its reliance on Tiversa Holding Corp., a cybersecurity firm that provided the FTC with the patient data file at the center of the case and whose credibility has been called into question during the course of the suit.

"Because this is the first case that challenged the FTC and won, the FTC is likely going to take that into consideration in future enforcement actions when deciding whether or not the facts are sufficient to move forward, and it will make them look at the facts and witnesses that are supportive of the enforcement actions a little harder," Robinson & Cole LLP partner Linn Freedman said.

The decision is also likely to give a boost to other businesses that may be targeted by the FTC down the road, according to attorneys.

“This could be the opening that leads to more companies, at least those with the resources, challenging other similar FTC enforcement actions in the future,” Shook Hardy & Bacon LLPdata security and privacy practice co-chair Al Saikali said.

The blow to the FTC’s authority could also have international ramifications, given that the commission has routinely asserted to its European counterparts concerned over the strength of the U.S. privacy regime that the regulator is an active and strong cop on the beat.

“This deflation of FTC power may have implications for international relations to the extent that the European Union and various data protection regulators may not be willing to defer to the FTC, which now looks like it can’t go much further than common law courts,” Neiditz said.

While the LabMD case is likely to have sweeping consequences, attorneys were quick to point out that the case is merely the first in what should be a long line of decisions that will shape the FTC’s data security authority.

Future case law is likely to come from not only cases that stem from companies now thinking about fighting rather than settling the commission’s data security claims, but also from the District of New Jersey, which is poised to rule on whether the FTC has met the harm threshold under Section 5 when it comes to its data security claims against Wyndham, whose conduct the commission has linked to three data breaches and $10.6 million in consumer harm.

“LabMD, to my mind, signals that courts are going to figure out the contours of actual and likely harm on a case-by-case basis, and after a few more cases with different factual scenarios, the scaffolding might become clearer,” Hart said.

LabMD is represented by Reed D. Rubinstein, William A. Sherman II and Sunni Harris ofDinsmore & Shohl LLP and Daniel Epstein and Patrick Massari of Cause of Action.

The FTC is represented by Alain Sheer, Laura Riposo VanDruff, Megan Cox, Ryan Mehm, John Krebs and Jarad Brown.

The case is In the Matter of LabMD Inc., docket number 9357, before the FTC's Office of the Administrative Law Judges.

--Editing by John Quinn and Mark Lebetkin.