WILMERHALE

LabMD Opinion Reverses ALJ Decision; Articulates Standard for "Substantial Injury" Under the Unfairness Prong of the FTC Act for FTC Data Security Actions

AUGUST 1, 2016

In a widely anticipated move, the Federal Trade Commission (FTC) has overruled a decision by its own Administrative Law Judge (ALJ) that had dismissed a case against a medical testing laboratory accused of unreasonable data security practices. The 37 page opinion continues the ongoing litigation between the FTC and the LabMD that began three years ago when the FTC alleged that LabMD's inadequate data security had allowed a patient insurance file to spread unprotected across a peer-to-peer file-sharing network. Last November, an ALJ held that the FTC had failed to prove that LabMD's lax security practices had actually harmed any consumers, but in Friday's opinion by Chairwoman Edith Ramirez, the FTC's commissioners unanimously concluded that the ALJ had applied the incorrect legal standard for unfairness under Section 5 of the FTC Act.

Describing LabMD's data security practices, the FTC's opinion explained how LabMD had failed to: (1) take reasonable steps to protect its computer network; (2) provide data security training to employees; or (3) adequately restrict or monitor its employees' use of its computer network. The opinion suggested that the problematic file-sharing network either never would have been installed on network computer or would never have "sat on the billing manager's computer for approximately three years," exposing the sensitive health records of 9,300 consumers, had proper security protocols been in place.

The FTC opinion provides considerable analysis into how the FTC evaluates unfairness in the context of data security. It explains how a business's poor data security practices often cannot be reasonably avoided by consumers and that the failure to have basic security in place cannot be outweighed by any countervailing benefits. However, the heart of the opinion is the Commission's discussion of what may constitute a "substantial injury" under Section 5 and, further, how a business's data security practices could be "likely to cause" such an injury.

Defining "Substantial Injury" Under Section 5

The FTC opinion fundamentally disagrees with the ALJ's holding that "privacy harms . . . unaccompanied by any tangible injury such as monetary harm or health and safety risks" may not constitute a "substantial injury" within the meaning of Section 5(n). Instead, the FTC found that the

unauthorized disclosure of sensitive health information was "in and of itself" a substantial injury.

The FTC opinion reiterated that the disclosure of sensitive information could cause "additional harms that are neither economic nor physical in nature but are nonetheless real and substantial and thus cognizable under Section 5(n)." The opinion notes that there is "broad recognition" in federal and state law that the disclosure of health information is inherently harmful, and it also highlights the FTC's first data security case against Eli Lilly as an example of where lax security resulted in the inadvertent disclosure of the email addresses of Prozac users.

Activities "Likely to Cause" Substantial Injury

In addition to holding that disclosure of sensitive information is a substantial injury, the FTC opinion also addressed whether the unauthorized exposure of records could also be “likely to cause substantial injury” under Section 5(n). The FTC’s initial allegation that the exposure of LabMD’s patient file on a file sharing network for more than eleven months was likely to meet this test, but the ALJ interpreted "likely to cause" as requiring a showing that a substantial injury was "probable" and not merely "possible." The FTC opinion rejects this analysis entirely.

First, the FTC opinion argues that both congressional intent and prior FTC enforcement actions demonstrate that the concept of risk is key to any analysis. Practices may be unfair even if the likelihood of an injury occurring is low if the magnitude of the potential injury is large. The opinion highlights the FTC’s action against International Harvester—"the quintessential unfairness case"—as standing for the proposition that a failure to warn of a "less than .001 percent" risk could be unfair where the resulting injuries might result in death or disfigurement. Describing both the sensitivity of information disclosed by LabMD and its attractiveness to identity thieves, the FTC held that there was significant risk of substantial injury in this case.

Moreover, the FTC opinion highlights the recent *Wyndham* decision by the Third Circuit Court of Appeals to support the notion that a risk analysis should inform whether a practice is likely to cause harm. While the Third Circuit held that defendants were liable for practices that were likely to cause substantial injury where customer harm was “foreseeable,” the FTC opinion notes that the Third Circuit’s analysis looked at both the “probability and expected size” of the potential harm when evaluating this. The Third Circuit concluded that unfair conduct can occur without an actual injury, and that Section 5 requires companies “to assess the risks that its actions could cause harm . . . and to implement reasonable measures to prevent or minimize such foreseeable harm.” According to the FTC opinion, LabMD’s activities were lacking in this regard.

Finally, the FTC opinion cautions that the ALJ's reasoning has the critical defect of reading the term "likely" out of the FTC's statutory authority. The ALJ had been critical of the FTC staff's failure to identify "even one consumer that suffered any harm" from LabMD’s action, but the FTC opinion explained that the FTC judges harmfulness not on the basis of actual future outcomes but the likelihood that a practice may be harmful at the time it occurs. "This is particularly true in the data security context," the opinion concludes.

What's Next?

The FTC opinion explores the how and why of LabMD's data security failings, and it reiterates the FTC's now standard expectations about reasonable data security. Interestingly, the FTC has also imposed a breach notification requirement in its order, requiring LabMD to notify affected individuals. The opinion is a powerful restatement of existing FTC thinking in the wake of *Wyndham*, but the case may yet be far from over. LabMD has sixty days to appeal the decision in a federal appellate court, and considering the course of the case thus far, it is likely that appeal will come soon.