

## No Harm? No Matter. FTC Broadens Data Security Liability

Article By:

David Heck

---

No harm, no foul? Not according to the FTC.

On July 29, 2016, the Commission held that a showing of tangible injury was not necessary in order for company acts and practices to be considered unfair. The case, [In the Matter of LabMD, Inc.](#), arose after a data security company accessed and downloaded a file from a former medical testing company, LabMD. The file contained 1,718 pages of personal information belonging to approximately 9,300 consumers, including names, addresses, dates of birth, social security numbers and medical information. The FTC's ruling overturned a [prior decision](#) by Chief Administrative Law Judge D. Michael Chappell, who had found that LabMD's supposed failure to institute reasonable data security measures was not likely to cause substantial injury to consumers.

In order to declare an act or practice unlawful on the grounds that it is unfair, the Federal Trade Commission Act requires a showing that (1) the act or practice causes or is likely to cause substantial injury to consumers; (2) the injury is not reasonably avoidable by consumers themselves; and (3) the benefits of the practice to consumers or competition do not outweigh the drawbacks. The FTC's complaint alleged that LabMD's lax security practices violated the FTC Act because, among other things, they failed to provide reasonable and appropriate security for personal information stored on LabMD's computer network and the company could have corrected the flaws at relatively low cost.

However, Judge Chappell never reached a conclusion on the reasonability of LabMD's security practices. Instead, he focused almost entirely on the first inquiry under the FTC Act, finding that there was no proof of tangible injury and that there was only a possibility of harm, rather than a probability.

"To impose liability for unfair conduct . . . where there is no proof of actual injury to any consumer, based only on an unspecified and theoretical 'risk' of a future data breach and identity theft injury, would require unacceptable speculation and would vitiate the statutory requirement of 'likely' substantial consumer injury." Judge Chappell noted that no harm had actually occurred in the seven years that the files were exposed and stated that fundamental fairness required a showing of more than "hypothetical or theoretical harm."

FTC Chairwoman Edith Ramirez disagreed. She and two other commissioners unanimously [concluded](#) that Judge Cappel used the wrong standard in determining the likelihood of harm. They determined that a practice could be unfair if the magnitude of the potential injury was large, even if the likelihood of an injury occurring was low. Further, the commissioners found that the FTC Act

---

allowed for “preemptive action,” meaning that no showing of actual harm was necessary.

While the commissioners conceded that cases of unfairness usually involved economic harm or physical health and safety risks, they found that these were not the only types of cognizable injuries under the FTC Act. Discussing medical information that included laboratory tests for HIV, herpes, prostate cancer, and testosterone levels, Chairwoman Ramirez wrote that the “privacy harm resulting from unauthorized disclosure of sensitive health or medical information is in and of itself a substantial injury.”

The commissioners then concluded that LabMD’s security practices were unreasonable and lacked “even basic precautions” that could protect against this type of injury. Among the more noteworthy deficiencies were the company’s failures to (1) use an intrusion-detection or file-monitoring system; (2) monitor traffic coming across its firewalls; (3) provide data security training to its employees; and (4) periodically delete consumer data that it had collected.

The ruling serves to highlight the breadth of the FTC’s enforcement powers and is significant because the FTC’s authority is rarely tested. Of the nearly 60 data security cases that have been brought by the FTC, only two have not settled. The other case that did not settle, which involved hotel chain Wyndham Worldwide Corp., also resulted in an expansion of the FTC’s powers. Wyndham challenged the FTC’s ability to pursue data security claims under its more conventional consumer-protection authority, but the Third Circuit Court of Appeals held last year that data security practices could be considered “unfair” under the FTC Act.

© 2025 Proskauer Rose LLP.

---

National Law Review, Volume VI, Number 216

Source URL: <https://natlawreview.com/article/no-harm-no-matter-ftc-broadens-data-security-liability>