WILLKIE FARR & GALLAGHER LLP

NEW YORK WASHINGTON HOUSTON PARIS LONDON FRANKFURT BRUSSELS MILAN ROME

CLIENT MEMORANDUM

FTC Finds "Harm" in LabMD Data Security Practices

August 1, 2016

AUTHORS

Daniel K. Alvarez | **James C. Dugan** | **Elizabeth J. Bower**

On July 29, 2016, the Federal Trade Commission (the "FTC" or "Commission") issued a much-anticipated Opinion and Final Order in *In the Matter of LabMD, Inc.*, a case involving a medical testing laboratory subject to an enforcement action under Section 5 of the Federal Trade Commission Act (the "FTC Act") for alleged lax data security practices. In a 37-page Opinion authored by Chair Edith Ramirez, the FTC reversed the order of an administrative law judge ("ALJ") dismissing the Commission's complaint against LabMD. Observing that the ALJ "applied the wrong legal standard for unfairness," the Commission concluded that LabMD's lax data security practices constituted "an unfair act or practice within the meaning of Section 5 of the FTC Act" by exposing consumers to substantial injury or a high likelihood of substantial injury. With this Opinion, the Commission dove head-first into the debate concerning the meaning of "harm" in the context of privacy and data security, offering a stark contrast to the position staked out in the Supreme Court's recent *Spokeo* decision. Further, the Commission's Opinion offers practical guidance on what the Commission considers reasonable data security practices.

Spokeo and Data Security Harms

As noted in our recent client memorandum, the LabMD case parallels in many respects the U.S. Supreme Court's decision in *Spokeo, Inc. v. Robins*.[1] In *Spokeo*, the Court opined that the "concreteness" requirement for Article III standing demands a showing of "*real* harm" or a "*material* risk of harm" in cases where plaintiffs allege harm will occur in the future. Further, while the Court acknowledged that "intangible injuries can nevertheless be concrete," it also stated that allegations of a "bare procedural violation" are insufficient to satisfy the concreteness prong of Article III standing. Though the Court stopped short of resolving an ongoing debate among the circuit courts about the nature of harm in privacy and data security cases, it clarified that courts must explicitly consider both the particularity and concreteness of the injuries alleged in such cases. Accordingly, *Spokeo* was widely perceived as having raised the bar to establish standing in cases involving intangible harm and risks of future harm, issues that are particularly germane to privacy and data security cases.

FTC Adopts New Substantial Injury Standard

The ALJ's decision in *LabMD* echoed the Supreme Court's reasoning in *Spokeo*, but the Commission rejected many of the ALJ's conclusions and distinguished *Spokeo*'s Article III analysis as having "no application" to the FTC's authority to bring enforcement actions under Section 5 of the FTC Act. Instead, the Commission offered its own definition of "harm" in privacy and data security cases by interpreting the meaning of "causes or is likely to cause substantial injury to consumers," as used within Section 5(n) of the FTC Act.

First, the Commission reiterated that a "substantial injury may be demonstrated by a showing of a small amount of harm to a large number of people, as well as a large amount of harm to a small number of people." The Commission also explained that even "subjective types of harm" may constitute a substantial injury. In particular, the Commission focused on the unique privacy and reputational harms associated with the disclosure of sensitive health and medical information. An unauthorized disclosure of which, it concluded, might result in "additional harms that are neither economic nor physical in nature but are nonetheless real and substantial and thus cognizable under Section 5(n)." Importantly, the Commission stated that these privacy and reputational harms are "*real* harms."

Second, the Commission determined that a future harm need not be "probable" to qualify as "likely to cause substantial injury" within the meaning of Section 5(n). Rather, the Commission concluded that Section 5(n) requires consideration of both the *likelihood* and potential *magnitude* of future harm. While a "significant risk" of injury may be sufficient to satisfy the requirements of Section 5(n), one may also satisfy the statute by showing the potential for a very serious injury even if there is a low risk that it may materialize. Under this reading, Section 5(n) requires only that there be a foreseeable risk of harm, and that the foreseeable risk be either highly likely or serious. This approach arguably establishes a lower bar than the "certainly impending" standard, and lower than what commentators have generally anticipated for Article III standing determinations after *Spokeo*.

[1] *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016).

Maintain Reasonable Data Security Practices

The Commission has brought nearly 60 data security cases to date. The vast majority of these cases have been settled,[2] and taken together these cases have provided informal guidance to industry with respect to what the Commission considers to be reasonable data security practices. However, *LabMD* represents the first time the full Commission has expounded upon both the definitional issues highlighted above and practical issues regarding what it believes to be reasonable data security practices within the context of a litigated case.[3] In the *LabMD* Opinion, the Commission listed the many basic security precautions LabMD failed to maintain. The Commission's Opinion should help guide Companies in developing and executing reasonable data security practices. Notably, however, the Opinion cited the FTC's past statement that

> [t]he touchstone of the Commission's approach to data security is reasonableness: a company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities. . . . [T]he Commission has made clear that it does not require perfect security; reasonable and appropriate security is a continuous process of assessing and addressing risks; there is no one-size-fits-all data security program; and the mere fact that a breach occurred does not mean that a company has violated the law.

Despite using the language of "reasonableness," the Commission – at least in the case of sensitive health information – seems to be measuring LabMD against a standard that is almost akin to strict liability. In particular, the Commission explained that the following security precautions are widely known and common industry practices that companies could adopt to maintain reasonable data security:

- **Employing adequate risk assessment tools**. Commonly used tools include intrusion detection systems, file integrity monitoring, and "penetration tests" that audit for industry-known software bugs.
- **Monitoring networks for unauthorized intrusion or exfiltration**. For example, review firewall logs or network activity logs.
- **Requiring strong passwords for employees to access the network**.
- **Conducting employee training on data security and privacy**. This training can include best practices and processes for reporting incidents.

---

[2] The Commission has litigated only two data security cases: *LabMD*, which went through the administrative process, and *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015), which went through the judicial process.

[3] In addition to this case and its earlier settlements, the Commission offers business guidance on data security that is a useful summation of its previous decisions.

- **Limiting access to personal information**. Not all employees need access to the personal data that a company collects. Ensure that mechanisms are in place that restrict access of personal data to those employees who need that access to perform their jobs.

- **Restricting or monitoring what employees download onto their work computers**. At a minimum, ensure that employees are trained about the risk of downloading certain types of files.

Next Steps

LabMD owner and CEO Michael Daugherty has already said that LabMD will appeal the Commission's decision. A petition for review with a U.S. Court of Appeals must be filed within 60 days. In the meantime, the *LabMD* Opinion sets a marker for how regulators and courts should think about harm in the context of data security, and reiterates the Commission's views on reasonable data security practices under Section 5 of the FTC Act.

Importantly, the *LabMD* and *Spokeo* cases occupy different areas of law. In particular, *LabMD* is distinguishable from *Spokeo* because the FTC does not have to establish standing in order to bring a lawsuit. Thus, *Spokeo* remains relevant in assessing cases brought by private litigants. This means that for the foreseeable future the definition of "harm" may be as much a function of the legal context in which the question is raised as it is a function of the acts of the parties involved.

We will continue to update you as this controversy moves forward.

If you have any questions regarding this memorandum, please contact Daniel K. Alvarez (202-303-1125; dalvarez@willkie.com), James C. Dugan (212-728-8654; jdugan@willkie.com), Elizabeth J. Bower (202-303-1252; ebower@willkie.com) or the Willkie attorney with whom you regularly work.

Willkie Farr & Gallagher LLP is an international law firm with offices in New York, Washington, Houston, Paris, London, Frankfurt, Brussels, Milan and Rome. The firm is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is (212) 728-8000 and our fax number is (212) 728-8111. Our website is located at www.willkie.com.

August 1, 2016