CARLTON FIELDS

Companies That Collect Sensitive Consumer Data Should Note the FTC's LabMD Ruling

CONSUMER FINANCE | CYBERSECURITY AND PRIVACY | HEALTH CARE | PHARMACEUTICALS AND MEDICAL DEVICES | TECHNOLOGY | AUGUST 1, 2016

Steven Blickensderfer

The FTC has been a leader in enforcing cybersecurity issues in recent years, and just last week it issued a highly-anticipated decision on its authority to regulate cybersecurity as a form of unfair consumer practice under Section 5 of the FTC Act. *See In re LabMD, Inc.* , FTC File No. 102-3099.

The FTC's July 28 opinion and order arose from its action against LabMD, a clinical lab that tested patient samples and collected/maintained sensitive personal information, including medical information. Between 2007-2008, LabMD experienced a data security incident that resulted in the exposure of sensitive health information of over 9,000 patients. The incident originated from an employee's installation of file-sharing software (LimeWire) onto a company computer that exposed sensitive medical information on a peer-to-peer network to millions of online users. The exposure went undetected for almost a year. LabMD never notified any consumers of the incident, and although some of the sensitive information reached the hands of identity thieves, there were no consumer complaints or actual harms associated with the disclosure.

Despite the absence of any actual harm to consumers, the FTC brought an enforcement action against LabMD arguing that its data security practices were unfair under Section 5. LabMD, in turn, challenged the FTC's authority to bring the action because it had not shown LabMD's data privacy practices caused or were likely to cause "substantial injury" to consumers, as Section 5 requires. In late 2015, an administrative law judge (ALJ) agreed with LabMD and dismissed the complaint, but the FTC commissioners reversed.

The FTC Interprets Section 5's "Substantial Injury" Requirement in Data Privacy Enforcement Actions

In its *LabMD* ruling, the FTC held that the ALJ employed an unduly stringent "substantial injury" standard under Section 5 of the FTC Act, and that it failed to appreciate that there were other forms of cognizable injury besides economic and physical harm. Drawing on its 1980 policy statement on the application of its unfairness authority, the FTC stated the following regarding the standard for showing data security practices caused or were likely to cause "substantial injury":

- "subjective types of harm" include "intangible but very real harm like privacy harm resulting from the disclosure of sensitive health or medical information";
- in determining whether a practice is "likely to cause substantial injury," the FTC looks to "the likelihood or probability of the injury occurring and the magnitude or seriousness of the injury if it does occur";
- showing a "significant risk" of injury at the time the breach occurred satisfies the "likely to cause" harm requirement; and
- Congress intended Section 5 to have a prophylactic purpose, which authorizes the FTC to address injuries that have "not yet manifested."

Applying the proper standard for substantial injury, as well as the other two prongs of the three-part unfairness test– (2) whether the alleged harm was reasonably avoidable by consumers; and, (3) whether it was outweighed by countervailing benefits to consumers – the FTC held that LabMD's conduct was "unfair." Consequently, LabMD, which is no longer in

business but maintains consumer data, is required to notify the affected consumers and implement a comprehensive privacy program to be in place for the next 20 years.

Lessons From the FTC's *LabMD* Ruling

Any company that collects and maintains sensitive consumer information, particularly regulated information such as health and financial data, should review the expansive LabMD decision, which offers the following lessons:

. The FTC's regulation of data security practices extends to situations that do not involve economic or physical consumer harm. Even if the risk of potential injury is low, the FTC may still find a data security practice unfair where the magnitude of the risk of potential injury is high.
. The FTC evaluates whether a data security practice will cause harm at the time the practice occurred, "not on the basis of actual future outcomes." As the FTC warned in its decision: "We need not wait for consumers to suffer known harm at the hands of identity thieves."
. To withstand scrutiny, the FTC recommends that a company's data security practices be reasonable and appropriate in light of the sensitivity and volume of the consumer information it maintains, the complexity of its business, and the cost of available the tools to improve security.

The three-commissioner FTC panel was unanimous in its decision, which can be found here.