FTC Establishes a Low Bar for Consumer Harm in Data Security Cases

Kevin L. Coy

On July 29, 2016, the Federal Trade Commission (FTC or "the Commission") issued an important opinion in its long-running data security case against LabMD, finding that the company engaged in unfair practices in violation of Section 5 of the Federal Trade Commission Act (FTC Act) as a result of poor data security practices.[1] In doing so, the Commission took an expansive view of what constitutes consumer harm in data security unfairness cases, finding that the unauthorized disclosure of sensitive health and medical information by itself constitutes a substantial injury. While health and medical information was at issue in the LabMD case, the FTC could also seek to apply the same principle to other types of sensitive data.

The Commission reversed the 2015 opinion of the Administrative Law Judge (ALJ) who had dismissed the case against LabMD, holding that FTC Complaint Counsel failed to demonstrate the requisite consumer harm because there was no proof that any consumers had been harmed. The Commission stated that the unauthorized disclosure of the information alone causes a substantial injury and that the Commission does not need to wait for harm to occur because "Section 5 very clearly has a 'prophylactic purpose' and authorizes the Commission to take 'preemptive action.' We need not wait for consumers to suffer known harm at the hands of identity thieves."[2]

LabMD has 60 days to appeal the Commission's decision to the Court of Appeals. If the Commission's Order stands, the decision, coupled with the FTC's win at the Third Circuit last year against Wyndham Hotels,[3] will give the FTC broad authority to bring data security cases without having to prove physical, economic, or even emotional harm to particular consumers. Instead, the FTC need only demonstrate that such harm is reasonably possible. The case also is noteworthy because, while LabMD is subject to HIPAA -- and action in such cases typically would be expected to come from the Office of Civil Rights at the Department of Health and Human Services -- the Commission brought its action under Section 5 of the FTC Act.

The backstory of the LabMD case is long and has taken many twists and turns. The central facts giving rise to the Commission's opinion, however, involve an incident in which the installation of file-sharing software on LabMD's system resulted in the exposure of a data file containing the medical and other sensitive personal information of 9,300 consumers on a peer-to-peer network accessible by millions of users for a period of 11 months during 2007-2008. The information exposed included names, dates of birth, Social Security numbers and codes for laboratory tests performed, including tests for HIV, herpes, prostate cancer, and testosterone levels. There was no proof that anyone accessed the file through the peer-to-peer network (other than a security firm that brought the matter to LabMD's attention and ultimately to the attention to the Commission) and no proof of actual physical, economic, or even emotional harm to particular consumers.

The question of consumer harm was central to the case. In order to prove an unfairness case under Section 5 of the FTC Act, it is necessary that the act or practice being challenged as unfair "causes 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 to

1 Federal Trade Commission, In the Matter of LabMD, Inc., a corporation (Docket No. 9357) (July 29, 2016) ("Commission Opinion").
2 *Id* at 23.
3 *Federal Trade Commission v. Wyndham Worldwide Corp. et. al.*, 799 F.3d 236 (3rd Cir. 2015).

competition."[4] The first prong of the test, whether the acts or practices of LabMD caused or is likely to cause substantial injury to consumers, was at the heart of the case. The ALJ found that Complaint Counsel had failed to prove that LabMD's actions caused or were likely to cause harm, and therefore dismissed the case. The ALJ opinion took the view that "[e]ven if there were proof of such harm, this would constitute only subjective or emotional harm that, under the facts of this case, where there is no proof of other tangible injury, is not a 'substantial injury' within the meaning of Section 5(n)."[5] The ALJ noted that there was no proof that anyone other than the security firm downloaded the exposed file, that there had been no consumer complaints or injuries linked to the exposure of the file, and that there was little likelihood that the information in the file would be redisclosed or would cause future harm.

The Commission reversed the ALJ on this critical element, holding that the ALJ applied the wrong legal standard. The Commission stated that, "In determining whether a practice is 'likely to cause a substantial injury,' we look to the likelihood or probability of the injury occurring and the magnitude or seriousness of the injury if it does occur. Thus, a practice may be unfair if the magnitude of the potential injury is large, even if the likelihood of the injury occurring is low."[6] The Commission looked to prior unfairness cases in other contexts, including a case where the Commission brought an unfairness action against a company for distributing razor blades in a manner that could make them accessible to small children even though no child had been injured and a case involving inadequate warnings on a tractor gas cap where the likelihood of harm was low, but harm, if it did occur, was substantial. "As is the case for analysis of unfairness generally, this evaluation does not require precise quantification. What is important is obtaining an overall understanding of the level of risk and harm to which consumers are exposed."[7] In the case of LabMD's breach, a file containing sensitive health information of 9,300 consumers was exposed to potential access for 11 months by millions of users of the file sharing service.

The Commission held that the potential harms from the exposure of the sensitive medical and other information, even absent proven economic or physical harm, was sufficient to satisfy the "cause or likely to cause substantial injury" standard, concluding "the disclosure of sensitive health or medical information causes additional harms that are neither economic or physical in nature but are nonetheless real and substantial and thus cognizable under Section 5(n)."[8] The Commission continued: "We conclude that the privacy harm resulting from the unauthorized disclosure of sensitive health or medical information is in and of itself a substantial injury under Section 5(n), and thus that LabMD's disclosure of the… file itself caused substantial injury."[9]

The Commission further found that showing a significant risk of injury satisfies the "likely to cause" standard. "When evaluating a practice, we judge the likelihood that the practice will cause harm at the time the practice occurred, not on the basis of actual future outcomes. This is particularly true in the data security context."[10] The Commission minimized the need to prove that the breach caused documentable harm: "Here given the absence of [breach] notification by LabMD, a lack of evidence regarding particular consumer injury tells us little about whether LabMD's security practices caused or were likely to cause substantial injury. Moreover, Section 5 very clearly has a 'prophylactic purpose' and authorizes the Commission to take 'preemptive action.' We need not wait for consumers to suffer known harm at the hands of identity thieves."[11]

The Commission also rejected LabMD's arguments that there should be an "injury in fact" standard, citing the Supreme Court's May 2016 opinion in *Spokeo v. Robins*.[12] The Commission stated "Standing has no application here, where the issue is the authority of an executive branch agency to enforce the law, rather than the authority of federal courts to entertain a private party's lawsuit.… Indeed, the 'injury in fact' prerequisite for standing is particularly inappropriate given Congress' empowerment of the FTC to 'tak[e] preemptive action,' consistent with 'Section 5's prophylactic purpose.'"[13]

4 15 U.S.C. § 45(n).
5 Commission Opinion at 7 (Citations omitted).
6 Commission Opinion at 10.
7 *Id.*
8 *Id.* at 17.
9 *Id.* at 19.
10 *Id* at 23.
11 *Id.*
12 136 S.Ct. 1540 (2016).
13 Commission Opinion at 20, n. 63 (Citations omitted).

While the Commission's Opinion is primarily important for the harm analysis discussed above, it also includes a detailed list of what the Commission found to be data security failings by LabMD in connection with the breach. As in other Commission data security cases, these failings are a useful check for other organizations regarding the Commission's expectations. In finding that LabMD engaged in unfair acts or practices in violation of Section 5, the Commission found that LabMD: [14]

- Failed to protect its computer network or employ adequate risk assessment tools;
  - Failed to use an intrusion detection system, file integrity monitoring, or penetration testing;
  - Neglected to monitor traffic coming across its firewalls;
  - Manual inspections were not used to detect security risks but rather to respond to employee complaints about computer performance;
  - Failed to consistently update anti-virus definitions or run and review anti-virus scans;
- Failed to provide data security training to its employees;
- Failed to adequately restrict and monitor the computer practices of individuals using its network;
  - Failed to adequately limit or monitor employee access to patients' sensitive information (and turned off some features in its laboratory software that would have restricted access by users);
  - Failed to adequately restrict or monitor what employees downloaded onto their work computers;
  - Gave management and sales employees administrative rights allowing them to change security settings and download software from the internet;
  - Failed to comply with internal policies that called for internal review of added or removed software; and
- Never deleted any of the consumer data that it collected.

The Commission's LabMD opinion is a reminder of the priority that the Commission places on data security matters for companies under its jurisdiction, even in the case of entities subject to HIPAA or other laws. It also underscores the Commission's intention to continue to be proactive in this area and not limit itself to cases where consumer harm occurs at the hands of identity thieves or others if a company is not adequately safeguarding sensitive personal data.

14 Commission Opinion at 11-16.

Authors and Contributors

Kevin L. Coy
Partner, DC Office
202.677.4034
kevin.coy@agg.com

not *if*, but *how*.®

About Arnall Golden Gregory LLP

Arnall Golden Gregory, a law firm with more than 150 attorneys in Atlanta and Washington, DC, employs a "business sensibility" approach, developing a deep understanding of each client's industry and situation in order to find a customized, cost-sensitive solution, and then continuing to help them stay one step ahead. Selected for The National Law Journal's prestigious 2013 Midsize Hot List, the firm offers corporate, litigation and regulatory services for numerous industries, including healthcare, life sciences, global logistics and transportation, real estate, food distribution, financial services, franchising, consumer products and services, information services, energy and manufacturing. AGG subscribes to the belief "not if, but how.®" Visit www.agg.com.

Atlanta Office
171 17th Street, NW
Suite 2100
Atlanta, GA 30363

Washington, DC Office
1775 Pennsylvania Avenue, NW
Suite 1000
Washington, DC 20006

To subscribe to future alerts, insights and newsletters: **http://www.agg.com/subscribe/**