Administrative Law Judge Rules Against FTC in Data Security Enforcement Action

By: Jay Shapiro and Jonathan D. Klein
Cyber Law and Data Protection Alert
11.19.15

The Federal Trade Commission's efforts to protect consumer data were dealt a blow this week by an administrative law judge in a landmark data security enforcement ruling. In a case that could reshape future Federal Trade Commission (FTC or the Commission) enforcement authority, FTC Chief Administrative Law Judge D. Michael Chappell dismissed the FTC's complaint against LabMD, a former medical testing company. Judge Chappell found that FTC's staff had failed to carry its burden of demonstrating a "likely substantial injury" to consumers resulting from LabMD's allegedly "unfair" data security practices. While Judge Chappell's decision represents a stunning defeat for the FTC and a major victory for LabMD as the first company to successfully challenge an FTC Section 5 data security enforcement proceeding, the ruling may be short-lived since FTC staff have the right, and are likely to, appeal the case to the full Commission, which will review the decision anew.

FTC Proceedings Against LabMD

The FTC's civil case against LabMD focused on two security incidents involving the alleged exposure of patient information from LabMD's network. In May 2008, Tiversa, a third-party cybersecurity consultant, informed LabMD that a 1,718-page insurance aging report was available on a peer-to-peer (P2P) file-sharing network through the LimeWire file-sharing application. That report allegedly contained names, dates of birth, Social Security numbers, and health insurance information of approximately 9,300 LabMD patients. After contacting LabMD, Tiversa subsequently provided information about the incidents to the FTC. The second alleged security incident occurred in October 2012, when Sacramento police officers found a small number of paper copies of LabMD "day sheets" and copied checks in the possession of individuals who subsequently plead guilty to identity theft charges. These documents included names and Social Security numbers.

The FTC filed a complaint against LabMD in August 2013 alleging that LabMD failed to employ reasonable and appropriate security measures to protect data on its networks, and that as a result of its "unreasonable" data security practices, consumers were at a risk of substantial injury. Thus, according to the complaint, LabMD's actions constituted an unfair practice under Section 5 of the FTC Act. LabMD contested the FTC allegations through the administrative process and parallel litigation, challenging the FTC's actions in federal court. The Eleventh Circuit eventually upheld the district court's dismissal of LabMD's complaint against the FTC in January 2015, finding that the complaint did not stem from a "final" agency action as required under the Administrative Procedure Act. Meanwhile, LabMD continued to pursue its challenge through the administrative process.

The administrative proceeding proved lengthy and contentious. With over 200 entries on the docket, the critical tactical mistake by the Commission appears to be the FTC's primary reliance on third-party evidence from Tiversa. In May 2015, during the course of the administrative proceedings, a Tiversa employee testified that Tiversa had fabricated evidence linking the LabMD insurance aging report to identity thieves' IP addresses nor had it ever found evidence that anyone other than LabMD or Tiversa had accessed the report. According to this witness, Tiversa fabricated this information and reported it to the FTC after it unsuccessfully sought to solicit business from LabMD. After this testimony, FTC staff indicated it would not rely on certain Tiversa-related testimony and evidence in its proposed findings of fact.

JUDGE CHAPPELL'S DECISION

Section 5(n) of the FTC Act provides that a practice can only be deemed "unfair" if: (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 injury is not outweighed by countervailing benefits to consumers or to competition. Although the statutory test for unfairness involves three elements, Judge Chappell focused almost exclusively on the first element, holding that the FTC failed to prove that this alleged unreasonable conduct caused or is likely to cause substantial injury to consumers. Judge Chappell noted that the FTC had proven the "possibility" of harm to consumers, but not any "probability," and Section 5 requires more than a hypothetical or theoretical harm to consumers for a finding of liability. Because the FTC failed to meet its burden under the first element, any factual determinations as to the additional two prongs was unnecessary.

With regard to the insurance aging report found on the P2P network, Judge Chappell determined that Tiversa was not a "credible" source of information with regard to the dissemination of this report. Instead, Judge Chappell found that the evidence failed to show that anyone besides Tiversa had ever downloaded this report through LimeWire (and that the FTC no longer even argued that anyone else had), and that the FTC staff failed to demonstrate that the "limited exposure" of this file had resulted, or could result, in any identity theft-related harm to consumers. Further, in his view, staff also failed to prove that consumers would likely suffer any "embarrassment or similar emotional harm" from the exposure of the file via P2P software alone. Even if staff had proven that consumers suffered "embarrassment" or "emotional harm," Judge Chappell noted that such harms would be "subjective" and would not meet the "substantial injury" standard set forth under Section 5(n).

IMPACT

In terms of federal agencies, the FTC has arguably become the most prominent and active cybersecurity enforcer to date, particularly because it has numerous enforcement mechanisms and broad enforcement authority over large swaths of the economy. With more than a decade of experience in data security matters, including nearly 60 data security enforcement matters, and a recent affirmation of its authority to pursue privacy and data security lapses under Section 5 in *FTC v. Wyndham Worldwide Corporation*, it is evident the FTC hoped to reap greater enforcement power through the LabMD matter. Unfortunately for the FTC, its own in-house judge decided otherwise, based in large part on its failure to ascertain credible evidence. The FTC's loss may certainly make future enforcement actions difficult for them as the standard for demonstrating "likely substantial harm" has been addressed in this ruling.

While this decision represents a victory for LabMD, in the face of a major setback to its data security enforcement under Section 5, FTC staff is likely to appeal this case before the full Commission. Nevertheless, even if a majority of the Commissioners reverse Judge Chappell's "likely harm" finding, in doing so the Commission could articulate a more precise standard for "likely substantial harm" under the first prong of the "unfairness" test that could guide future Section 5 jurisprudence. Should the Commission modify or reverse the findings and conclusions made by the administrative law judge, LabMD may finally have standing under the Administrative Procedure Act to appeal the final administrative decision in federal court and seek further review. Whether the now defunct company has the resources to take such action remains unclear, and, more importantly, so does the potential breadth of the impact of this ruling.

For additional information on this matter, please contact Jay Shapiro (shapiroj@whiteandwilliams.com | 212.714.3063), Jonathan Klein (kleinj@whiteandwilliams.com | 215.864.6887) or another member of the Cyber Law and Data Protection Group.