THE WALL STREET JOURNAL.

OPINION | COMMENTARY

Hounded Out of Business by Regulators

The company LabMD finally won its six-year battle with the FTC, but vindication came too late.

PHOTO: GETTY IMAGES/ISTOCKPHOTO

By **DAN EPSTEIN**

Nov. 19, 2015 7:11 p.m. ET

Sometimes winning is still losing. That is certainly true for companies that find themselves caught in the cross hairs of the federal government. Since 2013, my organization has defended one such company, the cancer-screening LabMD, against meritless allegations from the Federal Trade Commission. Last Friday, the FTC's chief administrative-law judge dismissed the agency's complaint. But it was too late. The reputational damage and expense of a six-year federal investigation forced LabMD to

close last year.

While the Atlanta-based company was in business, its work required securely storing personal-health data and medical records in compliance with Health and Human Services Department regulations under the Health Insurance Portability and Accountability Act, often known as HIPAA.

So it was alarming when, in May 2008, LabMD was contacted by Tiversa, a company that describes itself as a "world leader in P2P cyberintelligence," alleging that it had found on the Internet a LabMD insurance-agent file containing the names, dates of birth and Social Security numbers of about 9,000 patients. Oddly, Tiversa wouldn't disclose where or how it discovered the file. But the company demanded a fee of $40,000 to mitigate the situation.

After leading its own thorough review that turned up no sign that any patient information had been exposed online, LabMD refused to pay. Little did it know that this would lead to a yearslong fight with the federal government that would bring down the company.

Tiversa had an exploitation game going. The company would "scour" the IT networks of companies for confidential information, according to whistleblower testimony in May from Richard Wallace, a former forensic analyst at Tiversa. Upon finding any such information, Mr. Wallace said, Tiversa would contact the company and demand large payments to "fix" the problem.

If a company refused, Mr. Wallace testified, Tiversa would create IP addresses to match those that law enforcement had identified in other, unrelated proceedings as belonging to identity thieves, and then pretend that the information had spread to third parties across the Internet.

Tiversa has called Mr. Wallace's allegations "baseless" and attributed them to the complaints of a disgruntled former employee. The company is suing LabMD and Mr. Wallace for defamation.

In his May testimony, Mr. Wallace said that Tiversa's strategy was essentially, "Hire us or face the music." And that music, Mr. Wallace said, was the FTC. According to a January congressional investigation—the only way to know, as LabMD was denied discovery into this relationship—Tiversa began working closely with FTC staff in 2007.

As Mr. Wallace detailed in his testimony, and as was uncovered in the congressional investigation, two years later the FTC and Tiversa entered a deal wherein Tiversa would create a separate company that would pass to the agency confidential computer files it

had obtained from internal computer systems from LabMD and 88 other companies. The FTC then used the files to take enforcement action under Section 5 of the Federal Trade Commission Act for alleged unfair trade practices pertaining to inadequate data security. What specifically those inadequacies were, LabMD was not told.

Using Tiversa's information, and without ever confirming the veracity of its claims that the patient information was on the Internet—as the FTC admitted in court filings—the commission opened an investigation into LabMD in January 2010.

From the start, LabMD tried to cooperate. Yet the FTC refused to detail LabMD's data-security deficiencies and would not disclose the nature and extent of Tiversa's involvement. Eventually, the FTC demanded that LabMD sign an onerous consent order admitting wrongdoing and agreeing to 20 years of compliance reporting.

Unlike many other companies in similar situations, however, LabMD refused to cave and in 2012 went public with the ordeal. In what appeared to be retaliation, the FTC sued LabMD in 2013, alleging that the company engaged in "unreasonable" data-security practices that amounted to an "unfair" trade practice by not taking reasonable steps to protect patient information. FTC officials publicly attacked LabMD and imposed arduous demands on the doctors who used the company's diagnostic services. In just one example, the FTC subpoenaed a Florida oncology lab to produce documents and appear for depositions before government lawyers—all at the doctors' expense.

Yet after years of investigation and enforcement action, the FTC never produced a single patient or doctor who suffered or who alleged identity theft or harm because of LabMD's data-security practices. The FTC never claimed that LabMD violated HIPAA regulations, and until 2014—four years after its investigation began—never offered any data-security standards with which LabMD failed to comply.

The administrative-law judge's decision—which noted the lack of proof of a single victim in the case—vindicates LabMD, though Tiversa isn't admitting anything. "We have acted appropriately and legally in every way with respect to LabMD," the company said in a statement after last week's ruling.

But the case illustrates the injustice of the federal system that allows agencies to cow companies into submission rather than seek a day in court. During its three years of pre-suit investigation against LabMD, the FTC demanded thousands of documents, confidential employee depositions and several meetings with management. LabMD—which at its apex employed 30 people—spent hundreds of thousands of dollars meeting demands. No federal court would ever allow such abusive tactics. But this isn't federal court—it's a federal agency.

Furthermore, the FTC is likely to simply disregard the 92-page decision—which weighed witness credibility and the law—and side with commission staff. That's the still greater injustice: The FTC is not bound by administrative-law judge rulings. In fact, the agency has disregarded every adverse ruling over the past two decades, according to a February analysis by former FTC Commissioner Joshua Wright. Defendants' only recourse is appealing in federal court, a fresh burden in legal fees.

That's what happens when a federal agency serves as its own detective, prosecutor, judge, jury and executioner. As Mr. Wright observed, the FTC's record is "a strong sign of an unhealthy and biased institutional process." And he puts it perhaps most powerfully: "Even bank robbery prosecutions have less predictable outcomes than administrative adjudication at the FTC." Winning against the federal government should never require losing so much.

Mr. Epstein is the executive director of Cause of Action, a government watchdog. It represents LabMD.