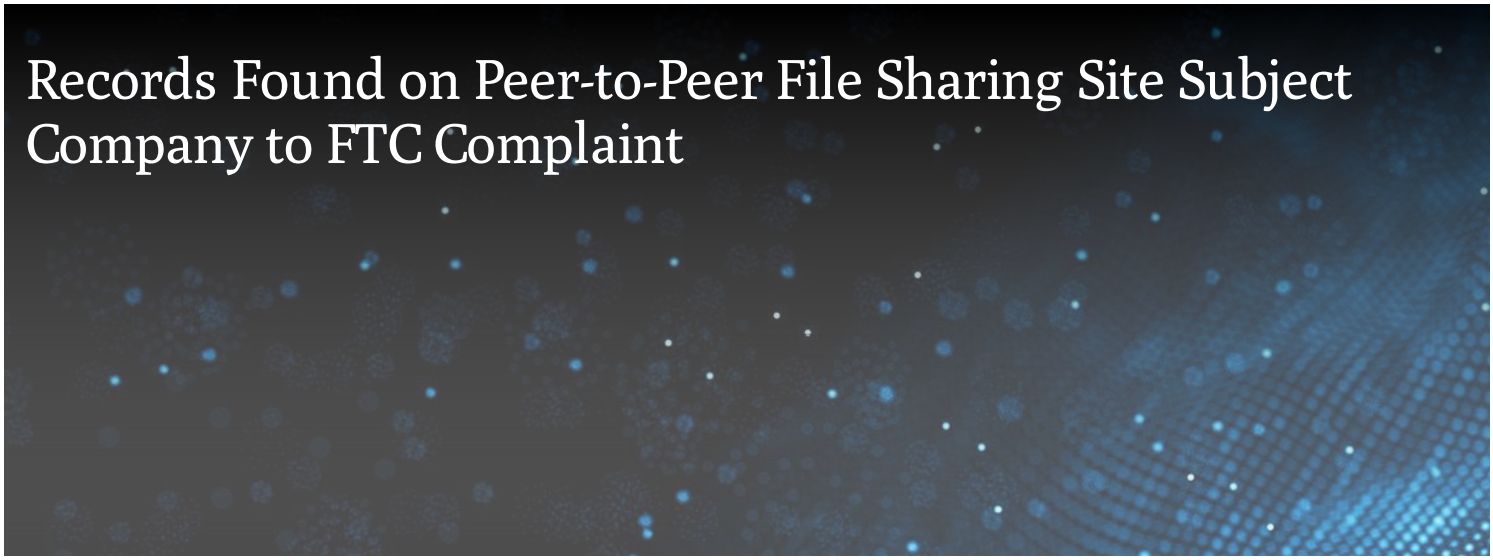
WINSTON & STRAWN LLP

BLOG

Records Found on Peer-to-Peer File Sharing Site Subject Company to FTC Complaint



SEPTEMBER 4, 2013

The Federal Trade Commission recently announced that it has filed a complaint against LabMD, a lab testing company, alleging that that the company failed to reasonably protect consumers' personal data after medical and other personal records of approximately 10,000 consumers were exposed. In the complaint, the FTC alleges that nearly 9,000 consumer records were found on a peer-to-peer file sharing network and that at least another 500 consumer records made their way into the hands of identity thieves. The FTC argued that LabMD failed to take "reasonable and appropriate measures" to protect consumer information, specifically alleging that it: 1) did not implement or maintain a comprehensive data security program to protect this information; 2) did not use readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities to this information; 3) did not use adequate measures to prevent employees from accessing personal information not needed to perform their jobs; 4) did not adequately train employees on basic security practices; and; 5) did not use readily available measures to prevent and detect unauthorized access to personal information. As part of the proposed order included in the complaint, LabMD would be required to implement a comprehensive data security program and have that program regularly reviewed by an independent expert. In addition, LabMD would have to notify all consumers whose information may have been accessible to unauthorized persons. Due to the sensitive nature of the documents provided to the FTC in connection with the investigation, the FTC has indicated that it will publicly release the complaint pending the resolution of any confidentiality claims.

TIP: This case is a reminder that the FTC will take action if it believes a company has failed to provide adequate security under the FTC Act, on the theory that such failure is an unfair or deceptive act. This case suggests that the FTC, in looking for what constitutes adequate security, will be looking at not just security programs, but also the effectiveness of those programs, and the existence of employee training and measures to detect incidents of unauthorized access.

This tip has been created for information and planning purposes. It is not intended to be, nor should it be, substituted for legal advice, which turns on specific facts.

2 Min Read

Related Locations

Chicago

Related Topics

Data Breach

Related Capabilities

Privacy & Data Security

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.