FTC Complaint Against Medical Laboratory Signals Agency's Continued Intent to Assert Authority in Data-Security-Breach Actions

In taking action against medical laboratory LabMD, the U.S. Federal Trade Commission demonstrated its continued intent to assert authority through the Federal Trade Commission Act in data-security-breach actions. On August 29, 2013, the FTC announced the filing of an administrative complaint alleging that LabMD failed to take reasonable measures to protect sensitive consumer information. The *LabMD* action is notable because almost all other actions in which the FTC has made similar allegations have settled without being litigated. The action may result in an administrative law judge ruling on the theory of liability advanced by the FTC in these prior cases, none of which has ever drawn a judicial opinion on the merits, and should accordingly be monitored closely by all companies that collect or use consumer information.

The FTC's complaint against LabMD, a cancer detection facility, is based on two instances in which LabMD purportedly exposed consumer information to risk of theft or misuse. The first alleged incident—which triggered the FTC investigation in 2010—was discovered when a LabMD spreadsheet was found on a peer-to-peer network. According to the FTC, the spreadsheet included personal information including names, Social Security numbers, dates of birth, and medical information. The second alleged incident occurred in 2012, when a local police department purportedly found LabMD documents in the possession of identity thieves. These documents, the FTC contends, also included names and Social Security numbers, as well as bank account information. The FTC claims that the two incidents combined involved the information of about 10,000 consumers.

The complaint, which has not yet been released publicly but is described in the FTC's press release, contains a proposed order that would require the implementation of a "comprehensive information security program" and biennial evaluations of the program by an independent consultant, for twenty years. The proposed order also includes a requirement, not typically included in FTC data security consent orders, that LabMD provide notice to consumers whose information LabMD has reason to believe was or could have been accessible to unauthorized persons and to consumers' health insurance companies.

LabMD has publicly vowed to aggressively defend the action. In a press statement, LabMD called the FTC action a "witch hunt" and declared the intention to "vigorously fight[] against the FTC's overreach." Through its actions during the pre-complaint investigation, LabMD has also demonstrated a willingness to fight vigorously. LabMD fought the perceived excess of the FTC investigation by challenging the FTC's Civil Investigative Demand—ultimately without success—both by petitioning the FTC to quash the CID and by defending an FTC suit in the Northern District of Georgia to enforce the CID. If there were any doubt of LabMD's disinclination to settle, it might be dispelled by the book, due out later this month, in which LabMD's founder and CEO recounts his experience with the FTC: *The Devil Inside the Beltway*.

LabMD's willingness to proceed in litigation makes the action worthy of note. The FTC's allegations against LabMD are themselves typical of many actions the FTC has brought against victims of data breaches. The theory set forth by the FTC is that the data breaches demonstrate the lack of reasonable security measures. This lack is then claimed to constitute an "unfair or deceptive" practice under the FTC Act. Despite the FTC's repeated use of this theory in dozens of complaints, however, the *LabMD* action is only the second data-security action in which the FTC has failed to achieve an early settlement, and no court or administrative law judge has ever ruled on the FTC's theory on the merits. The *LabMD* action demonstrates the FTC's

willingness to assert authority over data-security-breach matters even against defendants who are willing to challenge such authority.

The *LabMD* action and the FTC's stance that flaws in data security can constitute "unfair or deceptive" trade practices is of concern to all companies that collect or use consumer information. Such companies should assess the legal risks associated with their data-security practices and should monitor the FTC's activity in this area for further developments that might bear on these risks.

For more information regarding the *LabMD* action and its potential impact, please contact a member of our leading privacy and data security team, including Doug Meal, Mark Szpak, Jim DeGraw, and David McIntosh.