Gabriel (Gabe) Hamilton

Partner
208.383.3952
Boise
gahamilton@hollandhart.com

Recent FTC Action Emphasizes the Importance of Data Security in the Healthcare Industry

Insight — 08/12/2016

The Federal Trade Commission (FTC) recently delivered a fresh warning to the healthcare industry regarding the importance of data security — and the potential for regulatory enforcement actions against companies for lax security practices. In *LabMD*, the FTC found that a laboratory testing company had violated the FTC Act prohibition on unfair trade practices by failing to implement even the most basic data security practices.

Analysis of the Case

The FTC decision in the case of *LabMD, Inc*. is significant for two reasons.

1. FTC Has Overlapping Jurisdiction with HHS over the Data Security Practices of Healthcare Entities.

LabMD establishes that the FTC will assert jurisdiction over data security lapses by healthcare entities. This creates overlapping jurisdiction with the Department of Health and Human Services, which regulates the data security practices of healthcare entities under the HIPAA Security Rule.

2. Exposure of Consumers' Health Information Can Be an Unfair Practice Under the FTC Act Even If No Consumer Experiences Economic or Physical Harm as a Result.

LabMD reinforces the FTC's position that lax data security practices that expose highly sensitive consumer information—such as health information—can be “unfair” under the FTC Act regardless of whether any consumer suffers economic or physical harm as a result. In particular the FTC determined that exposure of consumer's health information both (a) creates a substantial injury to consumers, regardless of whether any consumer experienced tangible harm, based on the invasion of privacy and embarrassment and (b) is likely to cause substantial injury on the basis that the magnitude of the potential injury is great even if the probability of the injury occurring may be low. The FTC's position on this point is consistent with the position of other federal regulators, as we noted in a recent client alert.

Practical Takeaways

1. The HIPAA Security Rule Sets the Relevant Standard for Healthcare Entities.

A healthcare entity that makes good faith reasonable efforts to comply with

HIPAA is unlikely to run afoul of the FTC's much looser “reasonableness” standard. *LabMD* underscores the importance of maintaining robust data security practices that comply with the HIPAA Security Rule.

2. Security Breaches are Inevitable, Incident Response Is Critical.

The FTC noted in *LabMD* that “the mere fact that a breach occurred does not mean that a company has violated the law.” In other words, data breaches are now an inevitable fact of life that at best can be mitigated by data security practices. Entities that presumably have implemented robust, HIPAA compliant systems are frequently the victims of successful attacks. See, for example, the recent breach announced by Banner Health.

In this environment, defensive security measures are not enough. Data security programs must also include incident response plans that establish protocols for internal and external breach reporting, investigation, countermeasures, and communication with affected customers. The recent HIPAA guidance that ransomware attacks be treated as reportable breaches underscores the message: In addition to robust preventative measures, healthcare entities should be prepared with robust incident response plans.

3. Boards Should Prioritize Oversight of Data Security.

The final takeaway from *LabMD* relates to the conspicuous absence of LabMD's board of directors. In the entire 37 page FTC decision the board of directors is not mentioned once. This silence is damning. An engaged board of directors should (a) actively monitor the critical enterprise risks facing the business, such as data breach, and (b) set the tone at the top.

In a modern healthcare organization, data security is a critical area of enterprise risk and the board should be actively engaged in overseeing management's efforts to manage this risk. *LabMD* further confirms that the board of any organization that holds large amounts of consumer information, and particularly healthcare information, should consider oversight of data breach risk as equivalent in importance to oversight of financial reporting. An engaged, informed board would never have permitted LabMD to fail to implement data security practices that at the very least made a good faith effort to comply with the minimum requirements of the HIPAA Security Rule.

Further, a board that was consciously setting the tone at the top would not have tolerated the apparently careless attitude of senior management towards compliance and basic risk management. The most damning evidence against LabMD's board regarding its failure to set the tone at the top is that LabMD failed to follow its own written compliance procedures. Apparently the board paid so little attention to compliance that it did not require management to audit and report on the effectiveness of the compliance program.

Although the FTC's decision does not specifically call out the failures of LabMD board of directors, the case provides a powerful reminder of the ripple effect that corporate governance practices—whether good or bad—

have on an organization.

Subscribe to get our Insights delivered to your inbox.