Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Fitbit's IPO Is An Exercise In Disclosing Data Risks

By **Allison Grande**

Law360, New York (May 27, 2015, 5:07 PM ET) -- Fitness-tracking company Fitbit Inc.'s exhaustive disclosure of potential cybersecurity risks to the troves of personal data it collects highlights the importance of making tailored statements leading up to an initial public offering that could prove vital in staving off future scrutiny from regulators and shareholders.

In filing for an IPO of up to $100 million earlier this month, the San Francisco-based maker of activity and fitness-tracking devices in its S-1 filing with the U.S.Securities and Exchange Commission laid out risk factors related to not only the pressures of the emerging connected device market, but also those tied to the increasing prevalence of data losses and intrusions.

While publicly traded companies have been on notice since 2011 that their material risk disclosures need to include both threats to their security as well as breach incidents, businesses just coming to the market, especially those that amass vast consumer data sets and are connected to the emerging "Internet of Things," are quickly learning that a vital piece of the public offering process is to craft clear and relevant cyberrisk disclosures.

"It's clear that if a company intends to go public, it should expect to and prior to taking this step should be in a position to comply with the SEC guidance related to cyberrisk disclosures," Quarles & Brady LLP commercial law team leader Jessica Franken said. "While the SEC doesn't govern them publicly until the time they go public, it doesn't hurt to take off the training wheels and act like they're already public."

According to the staff-level disclosure guidance issued by the SEC four years ago, public companies must disclose cybersecurity risks and incidents that could have a material impact on their bottom line.

The disclosure practice has gained significant traction and attention in recent years, as businesses begin to scoop up more consumer data and reports of data breaches become more widespread, making it imperative that newly public companies think carefully about their cyberrisks before coming to market and provide timely and accurate information about cyberthreats and risks that a reasonable investor would consider important, attorneys say.

"Cybersecurity has been a growing concern, garnering significant public and governmental awareness, as well as attention at both the board of director and investor levels," Mayer Brown LLP counsel Laura Richman said. "As a result of increasing sensitivity over the pervasiveness of cyber incidents, there may be a heightened scrutiny of cybersecurity disclosures."

For companies coming to market, the most scrutiny is likely to come from not only the SEC, which could offer feedback on the disclosures prior to finalizing their prospectus, but also shareholders who claim to have been harmed by a breach that was caused by a risk factor they claim a company failed to disclose.

“Businesses need to make sure that they are not overlooking risk factors because the disclosures they make could be an insurance policy of sorts when defending claims over a breach, if the breach occurs in exactly the way that a company described it could happen,” Covington & Burling LLP partner Keir Gumbs said.

The disclosure could be particularly useful in fending off class actions, which typically hinge on the premise that the public had no warning of a particular risk factor that led to a data loss, attorneys noted.

“Plaintiffs are having some success arguing, after a breach, that the companies never adequately disclosed what information they were collecting and what they were doing with it, and that failure to disclose, more so than the breach itself, becomes the ‘bad act’ and the focus of the lawsuit,” Shook Hardy & Bacon LLP data security and privacy practice co-chair Al Saikali said. “A full and accurate disclosure helps minimize this risk.”

Given the boost that properly crafted disclosures could present to combating future liabilities, businesses need to ensure that they have a strong grasp on how the cyberrisks inherent in their specific sector apply to their business model, attorneys say.

“The SEC has made it pretty clear that cyber disclosures need to be tailored for your business, and that boilerplate disclosures are going to be frowned upon,” Mintz Levin Cohn Ferris Glovsky & Popeo PC privacy and security practice chairwoman Cynthia Larose said. “Companies need to be doing a complete internal risk assessment to determine what their specific risks are, and should be able to apply that in a way that tells investors what they need to know without providing a roadmap to those that might want to harm companies.”

In its S-1 filing, Fitbit hit on the major cybersecurity risk factors that have been previously flagged by the SEC, including vulnerabilities created by its governmental obligations and other legal obligations related to privacy, the “volume and sensitivity” of the personal and health information it collects, and its use of third-party vendors.

“What the company has done is picked off major categories of risk and tried to build it around the uniqueness of their industry in effect, but at the same time they tried to remain general,” Reed Smith LLP counsel Sarah Wolff said.

But while the Fitbit disclosure appears to broadly cover risks, its lack of granularity — for example, its failure to disclose its vetting process for third-party vendors — could open it up to liability down the road, attorneys said.

“Although it is noteworthy that Fitbit included a disclosure about potential cyberrisks in its S-1, it is unclear if such a general disclosure will protect Fitbit from ‘Monday night quarterbacking’ by claimants, after an unexpected cyberbreach has taken place,” said Hsiao "Mark" Mao, vice chairman of Kaufman Dolowich & Voluck LLP'stechnology services practice. “One only needs to read the derivative lawsuits filed against Target’s officers ... to realize that."

Though the contents of a bullet-proof disclosure will vary by industry and change over time, attorneys advise companies filing for IPOs or revamping their business models in a way that could increase their consumer data consumption to ensure they've thoroughly considered their cyberrisk profile to avoid surprises down the road.

“Realistically, the risk factor section shouldn’t be generalized,” Gumbs said. “It’s not unusual for companies in the same industry to have common risks, but at the end of the day, a company’s disclosure should be specific enough to help investors.”

--Editing by John Quinn and Emily Kokoll.

All Content © 2003-2015, Portfolio Media, Inc.