Facebook Fined Again: Real Hypothetical Risks

August 15, 2019 Matthew Fry

PRACTICES Corporate, Capital Markets and Securities

On July 24, 2019, the Securities and Exchange Commission (the "***SEC***") announced charges alleging that Facebook, Inc. ("***Facebook***") made misleading public disclosures in its risk factors regarding the hypothetical risk of misuse of user data after becoming aware that user data had actually been misused. Facebook agreed to pay a $100 million civil penalty to settle the charges without admitting or denying the SEC's factual allegations. The penalty followed Facebook's settlement with the Federal Trade Commission (the "***FTC***") under which Facebook agreed to pay a record $5 billion penalty for an alleged violation of a prior FTC consent decree related to data misuse.

The SEC's complaint alleged that in 2015 Facebook became aware that Cambridge Analytica, a third-party developer, had misused Facebook user data in violation of Facebook's third-party terms and conditions. The SEC's complaint further asserted that Facebook failed to supplement its public disclosures related to data misuse for over two years after becoming aware of the incident. Facebook's risk factor disclosures merely presented the risk of misuse of user data as hypothetical, stating, "our data or our users' data *may* be improperly accessed, used or disclosed" (emphasis added), when Facebook employees knew that user data had already been misused by Cambridge Analytica. Facebook's stock price declined following public disclosure of the data misuse in March 2018.

In its public announcement regarding the charges, Stephanie Avakian, co-director of the SEC's Enforcement Division, stated, "Public companies must have procedures in place to make accurate disclosures about material business risks." According to the SEC, the hypothetical phrasing of a risk can create the misleading impression that such a risk has not occurred. The SEC also noted that Facebook lacked sufficient policies and procedures designed to evaluate data breach or related investigations for the purpose of determining disclosure obligations.

Last year in a similar action, Altaba, formerly known as Yahoo!, paid a $35 million penalty to settle SEC charges that Altaba failed to update a data breach risk factor during the two years following a major data breach involving the theft of user information. Altaba's filings stated only that it faced the risk of, and negative effects that might flow from, data breaches, even though it knew that a significant data breach had occurred.

Issuers should take notice of these settlements and use them as a reminder to perform regular reviews of their risk factors, supplementing hypothetical risks with descriptions of any factual circumstances where those hypothetical risks have occurred.[1] As part of this process, issuers should review and update their disclosure controls and procedures, which should be sufficiently broad enough to identify and assess risks and actual incidents that impact their disclosure obligations. Disclosure controls and procedures should ensure that information potentially subject to required disclosure is brought to the attention of the individuals who are primarily responsible for drafting and approving SEC reports. Issuers should also consider sharing information concerning incidents with outside disclosure counsel to evaluate their disclosure obligations, which the SEC indicated Facebook failed to do.

For additional information, including guidance regarding disclosure obligations, please contact any member of Haynes Boone's Capital Markets and Securities practice group.

---

[1] As part of these routine reviews, issuers should consult the SEC cybersecurity guidance issued on February 21, 2018 (found here) which, among other items, discusses factors to be weighed when considering whether even immaterial incidents should be disclosed to place risk factor disclosures in proper context. Please also see our prior client alert (found here) discussing the cybersecurity guidance.