Yahoo! Settlement Affirms SEC's Focus on Cybersecurity Disclosures

05.04.2018

In late April 2018, the SEC and Altaba (formerly known as Yahoo!) agreed to a $35 million penalty to settle charges that Yahoo! misled investors by failing to disclose to investors its December 2014 data breach in which hackers stole personal data relating to hundreds of millions of user accounts[1]

The SEC's order finds that, despite its knowledge of the massive 2014 data breach, Yahoo! did not disclose the breach in its securities filings for nearly two years. As a result, Yahoo!'s public disclosures were materially misleading and violated various provisions of the Securities Act of 1933 and the Securities Exchange Act of 1934. More specifically, (i) Yahoo!'s risk factor disclosures spoke only to the risk of potential future data breaches that might expose the company to loss of its users' personal information and the attendant consequences, without disclosing that the data breach had in fact already occurred, (ii) its MD&A omitted known trends or uncertainties related to liquidity and net revenue in connection with the breach and (iii) a 2016 stock purchase agreement attached as an exhibit to a Form 8-K filed by Yahoo! contained affirmative representations denying the existence of any significant data breaches. The latter point also reinforces the SEC's view that representations and warranties made in material contracts filed with the SEC constitute public disclosure under federal securities laws and, as such, could be misleading if additional material facts exist that contradict or qualify those representations.

Finally, the SEC's order finds that Yahoo! failed to maintain disclosure controls and procedures designed to ensure that reports from Yahoo!'s information security team concerning cyber breaches, or the risk of such breaches, were properly and timely assessed for potential disclosure.

The Yahoo! order affirms the SEC's focus on cybersecurity disclosures and builds upon the SEC's new cybersecurity guidance from February of this year.[2] Among other things, that guidance encouraged companies to avoid generic disclosure and include specific information as to a company's particular cybersecurity incidents and risk profile (including, for example, consideration of prior incidents, the probability and magnitude of future incidents, costs of prevention or remediation, and reputational harm, particularly in the risk factors and MD&A) and stressed the need for expanded disclosure controls and procedures that function effectively to collect cybersecurity-related information and facilitate its timely analysis by responsible personnel.

In light of these developments, companies are reminded to:

- Reexamine the company's cybersecurity-related disclosure to ensure that such disclosures are appropriately tailored, among other considerations, to a company's particular cybersecurity risks, the potential costs and other consequences of such risks, and the impact of any known trends and uncertainties relating to actual cyber hacks and vulnerabilities.

- Evaluate whether disclosure controls and procedures include appropriate notification of information regarding potential breaches or risks to senior leaders to facilitate the timely materiality assessment necessary to comply with their disclosure obligations under the federal securities laws.

- Review and revise codes of ethics and insider trading policies and procedures to address actual or suspected cybersecurity incidents as potentially material non-public information.

[1] The order is available at: https://www.sec.gov/litigation/admin/2018/33-10485.pdf.

[2] The guidance is available at: https://www.sec.gov/rules/interp/2018/33-10459.pdf.

Related People

- Lee G. Lester – 804.420.6583 – llester@williamsmullen.com

Related Services

- Securities & Corporate Governance
- Corporate
- Data Protection & Cybersecurity