Articles + Publications | May 1, 2018

Locke Lord QuickStudy: An Unasserted Lesson of the SEC's Yahoo Cyberbreach Enforcement Action

WRITTEN BY

Stanley Keller

Much has already been written about the SEC's enforcement action involving Yahoo's failure to adequately disclose a cyberbreach.[1] I am writing about something that the SEC's announcement and order did not address and therefore has not been written about.

On April 24, 2018, the SEC announced a settlement with Altaba Inc., which formerly was Yahoo! Inc., under which Altaba agreed to pay $35 million and take certain remedial actions to resolve claims that Yahoo violated the federal securities law by failing to make timely disclosures until September 2016 related to a 2014 data breach of its user database.[2] The SEC's announcement and order focused (i) on Yahoo's misleading risk factor, noting that identifying the potential of future data breaches is misleading when a material one has already occurred, (ii) on the failure to disclose the consequences of the data breach as a known trend and uncertainty in MD&A, and (iii) on the misrepresentation arising from a representation as to the absence of data breaches in a merger agreement filed as an exhibit to an Exchange Act report.[3] The SEC also noted the deficiency in Yahoo's disclosure controls and procedures, indicating that the procedures were insufficient to ensure that cyber events identified by the information technology officials were appropriately evaluated for potential disclosures.[4]

The SEC's Yahoo enforcement action did not address the failure of Yahoo's financial statements to include disclosure (and possibly an accrual) under Accounting Standards Codification 450-20 for the potential loss contingencies resulting from the 2014 data breach. Not much imagination typically is required to foresee the potential for significant liabilities arising from a massive cyberbreach and therefore the importance of considering the financial statement implications of that breach among other required disclosures. In this respect, the Yahoo enforcement action has similarities to the 2017 SEC enforcement action against General Motors for inadequate accounting controls that prevented GM from properly assessing the impact on its financial statements of its defective ignition switch problems.[5] Both actions provide the same lesson regarding the need for proper controls so that operational problems, like cyberbreaches and defective ignition switches, in addition to the more obvious litigation matters, are brought to the attention of the company officials in a position to evaluate the need for disclosure and the impact on the financial statements.

In both the Yahoo and GM actions, the loss contingencies involved unasserted claims that, under ASC 450-20, required an assessment as to whether claims were probable and, if so, whether a material loss was reasonably possible (i.e., more than remote). If this test is met, disclosure is required, with a quantification of the estimated loss or range of loss if an estimate can be made. In addition, if the loss is both probable and can be estimated, the estimated amount must be accrued as a charge to income. Applying ASC 450-20 to these types of situations can involve difficult judgments and the SEC indicated in its announcement of the Yahoo settlement that it does not

©2026 Troutman Pepper Locke

second guess good faith exercises of judgment about cyber-incident disclosure. However, companies need to make reasonable efforts to meet their cyber and other loss contingency disclosure and accounting obligations and to document those efforts and the basis of their judgments. These efforts should include having in place comprehensive disclosure controls and procedures and accounting controls that are documented and periodically reviewed and assessed for compliance.

—

[1] Altaba Inc., f/d/b/a Yahoo! Inc., Securities Act Release No. 10485, Exchange Act Release No. 83096, Accounting and Auditing Enforcement Release No. 3937, Administrative Proceeding File No. 3973 (Apr. 24, 2018).

[2] Press Release, SEC, Altaba, Formerly Known As Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees To Pay $35 Million (Apr. 24, 2018).

[3] See my article, Keller and Held, "The Meaning of the Titan 21(a) Report: New Disclosure Practices for Contractual Representations," INSIGHTS, Vol. 19, No. 6, June 2005 at p. 2.

[4] The Yahoo enforcement action needs to be read together with the SEC's recent interpretive guidance on cybersecurity disclosure since it is obvious that each influenced the other. See SEC, Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Release Nos. 33-10459, 34-82746 (Feb. 26, 2018).

[5] General Motors Company, Exchange Act Release No. 79825, Accounting and Auditing Enforcement Release No. 3850, Administrative Proceeding File No. 3-17797 (Jan. 18, 2017).

RELATED INDUSTRIES + PRACTICES

- Capital Markets