ALERT MEMORANDUM

Yahoo's Successor Settles First-Ever Case Involving SEC Charges for Failing to Disclose a Cybersecurity Incident

April 27, 2018

On April 24, 2018, Altaba, formerly known as Yahoo, entered into a settlement with the Securities and Exchange Commission (the "SEC"), pursuant to which Altaba agreed to pay $35 million to resolve allegations that Yahoo violated federal securities laws in connection with the disclosure of the 2014 data breach of its user database. The case represents the first time a public company has been charged by the SEC for failing to adequately disclose a cyber breach, an area that is expected to face continued heightened scrutiny as enforcement authorities and the public are increasingly focused on the actions taken by companies in response to such incidents. Altaba's settlement with the SEC, coming on the heels of its agreement to pay $80 million to civil class action plaintiffs alleging similar disclosure violations, underscores the increasing potential legal exposure for companies based on failing to properly disclose cybersecurity risks and incidents.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors:

WASHINGTON

Matthew C. Solomon
+1 202 974 1680
msolomon@cgsh.com

NEW YORK

Pamela L. Marcogliese
+1 212 225 2556
pmarcogliese@cgsh.com

Rahul Mukhi
+1 212 225 2912
rmukhi@cgsh.com

Kal Blassberger
+1 212 225 2112
kblassberger@cgsh.com

Background

As alleged, Yahoo learned in late 2014 that it had recently suffered a data breach affecting over 500 million user accounts (the "2014 Breach"). Yahoo did not disclose the 2014 Breach until September 2016. During the time period Yahoo was aware of the undisclosed breach, it entered into negotiations to be acquired by Verizon and finalized a stock purchase agreement in July 2016, two months prior to the disclosure of the 2014 Breach. Following the disclosure in September 2016, Yahoo's stock price dropped 3% and it later renegotiated the stock purchase agreement to reduce the price paid for Yahoo's operating business by $350 million.

In or about late 2016, following its disclosure of the 2014 Breach, Yahoo learned about a separate breach that had taken place in August 2013 and promptly announced that such breach had affected 1 billion users (the "2013 Breach"). In October 2017, Yahoo updated its disclosure concerning the 2013 Breach, announcing that it now believed that all 3 billion of its accounts had been affected.

The Settlement

Altaba's SEC settlement centered on the 2014 Breach only. The SEC found that despite learning of the 2014 Breach in late 2014—which resulted in the theft of as many as 500 million of its users' Yahoo usernames, email addresses, telephone numbers, dates of birth, hashed passwords, and security questions and answers, referred to internally as Yahoo's "crown jewels"—Yahoo failed to timely disclose the material cybersecurity incident in any of its public securities filings until September 2016. Although Yahoo senior management and relevant legal staff were made aware of the 2014 Breach, according to the SEC, they "did not properly assess the scope, business impact, or legal implications of the breach, including how and where the breach should have been disclosed in Yahoo's public filings or whether the fact of the breach rendered, or would render, any statements made by Yahoo in its public filings misleading."[1] The SEC also faulted Yahoo's senior management and legal staff because they "did not share information regarding the breach with Yahoo's auditors or outside counsel in order to assess the company's disclosure obligations in its public filings."[2]

Among other things, the SEC found that Yahoo's risk factor disclosures in its annual and quarterly reports from 2014 through 2016 were materially misleading in that they claimed the company only faced the risk of potential *future* data breaches, without disclosing that "a massive data breach" had in fact already occurred.[3] The SEC also alleged that Yahoo management's discussion and analysis of financial condition and results of operations ("MD&A") in those reports was also misleading to the extent it omitted known trends or uncertainties with regard to liquidity or net revenue presented by the 2014 Breach.[4] Finally, the SEC further found that Yahoo did not maintain adequate disclosure controls and procedures designed to ensure that reports from Yahoo's information security team raising actual incidents of the theft of user data, or the significant risk of theft of user data, were properly and timely assessed to determine how and where data breaches should be disclosed in Yahoo's public filings.[5]

Based on these allegations, the SEC found that Yahoo violated Sections 17(a)(2) and 17(a)(3) of the Securities Act and Section 13(a) of the Securities Exchange Act.[6] To settle the charges, Altaba, without admitting or denying liability, agreed to cease and desist from any further violations of the federal securities laws and pay a civil penalty of $35 million.

[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. 3937 (Apr. 24, 2018) at ¶ 14.

[2] *Id.* at ¶ 15.
[3] *Id.* at ¶¶ 2, 16.
[4] *Id.*
[5] *Id.* at ¶ 15.
[6] *Id.* at ¶¶ 22-23.

Takeaways

There are several important takeaways from the settlement:

— *First*, public companies should take seriously the SEC's repeated warnings that one of its top priorities is ensuring that public companies meet their obligations to adequately disclose material cybersecurity incidents and risks. This requires regular assessment of cyber incidents and risks in light of the company's disclosures, with the assistance of outside counsel and auditors as appropriate, and ensuring that there are adequate disclosure controls in place for such incidents and risks.

— *Second*, the SEC's recently released interpretive guidance on cybersecurity disclosure is an important guidepost for all companies with such disclosure obligations. The guidance specifically cited the fact that the SEC views disclosure that a company is subject to *future* cybersecurity attacks as inadequate if the company had *already* suffered such incidents. Notably, the Yahoo settlement specifically faulted the company for this precise inadequacy in its disclosures. Similarly, the recent guidance encouraged companies to adopt comprehensive policies and procedures related to cybersecurity and to assess their compliance regularly, including the sufficiency of their disclosure controls and procedures as they relate to cybersecurity disclosure. The Yahoo settlement also found that the company had inadequate such controls.

— *Third*, at the same time the SEC announced the settlement, it took care to emphasize that "[w]e do not second-guess good faith exercises of judgment about cyber-incident disclosure."[7] The SEC went on to note that Yahoo failed to meet this standard with respect to the 2014 Breach, but by articulating a "good faith" standard the SEC likely meant to send a message to the broader market that it is not seeking to penalize companies that make reasonable efforts to meet their cyber disclosure obligations.

— *Fourth*, it is also notable that the SEC charges did *not* include allegations that Yahoo violated securities laws with respect to the 2013 Breach. Yahoo had promptly disclosed the 2013 Breach after learning about it in late 2016, but updated its disclosure almost a year later with significant new information about the scope of the breach. The SEC's recent guidance indicated that it was mindful that some material facts may not be available at the time of the initial disclosure, as was apparently the case with respect to the 2013 Breach.[8] At the same time, the SEC cautioned that "an ongoing internal or external investigation – which often can be lengthy – would not on its own provide a basis for avoiding disclosures of a material cybersecurity incident."[9]

— *Finally*, it is worth noting that the Commission did not insist on settlements with any

[7] Press Release, SEC, Altaba, Formerly Known As Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees To Pay $35 Million (Apr. 24, 2018), https://www.sec.gov/news/press-release/2018-71.

[8] As we have previously discussed, the federal securities laws do not impose a general affirmative duty on public companies to continuously disclose material information and, as acknowledged in Footnote 37 of the interpretive guidance, circuits are split on whether a duty to update exists. However, in circuits where a duty to update has been found to exist, a distinction has often been drawn between statements of a policy nature that are within the company's control and statements describing then current facts that would be expected to change over time. The former have been held subject to a duty to update while the latter have not. *See In re Advanta Corp. Securities Litigation*, 180 F.3d 525, 536 (3d Cir. 1997) ("[T]he voluntary disclosure of an ordinary earnings forecast does not trigger any duty to update."); *In re Burlington Coat Factory Securities Litigation*, 114 F.3d 1410, 1433 (3d Cir. 1997); *In re Duane Reade Inc. Securities Litigation*, No. 02 Civ. 6478 (NRB), 2003 WL 22801416, at *7 (S.D.N.Y. Nov. 25, 2003), *aff'd sub nom. Nardoff v. Duane Reade, Inc.*, 107 F. App'x 250 (2d Cir. 2004) ("'company has no duty to update forward--looking statements merely because changing circumstances have proven them wrong.'").

[9] See SEC, Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg 8166, 8169 (Feb. 26, 2018), https://www.federalregister.gov/documents/2018/02/26/2018-03858/commission-statement-and-guidance-on-public-company-cybersecurity-disclosures.

individuals. Companies, of course, can only commit securities violations through the actions of their employees. While it is not unusual for the Commission to settle entity-only cases on a "collective negligence" theory, the SEC Chair and the Enforcement Division's leadership have emphasized the need to hold individuals accountable in order to maximize the deterrent impact of SEC actions.[10]

Click here for our prior memorandum on the SEC's recent cybersecurity interpretive guidance and here for our discussion on the SEC's cyber unit.

…

CLEARY GOTTLIEB

[10] *See, e.g.*, Steven R. Peikin, Co-Director, Div. Enf't., SEC, Reflections on the Past, Present, and Future of the SEC's Enforcement of the Foreign Corrupt Practices Act, Keynote Address at N.Y.U. Program on Corporate Law and Enforcement Conference: No Turning Back: 40 Years of the FCAP and 20 Years of the OECD Anti-Bribery Convention Impacts, Achievements, and Future Challenges (Nov. 9, 2017), https://www.sec.gov/news/speech/speech-peikin-2017-11-09; SEC Div. Enf't., Annual Report A Look Back at Fiscal Year 2017, at 2 (Nov. 15, 2017), https://www.sec.gov/files/enforcement-annual-report-2017.pdf.