# Altaba (Yahoo) Agrees to Pay $35 million Penalty as SEC Continues to Emphasize Importance of Cybersecurity Data Breach Disclosures

Brian A. Teras, B. Joseph Alley, Jr., and Kevin L. Coy

On April 24, 2018, the Securities and Exchange Commission (the "SEC") announced[1] that Altaba Inc. (f/k/a Yahoo! Inc.) agreed to pay a $35 million penalty relating to charges that it misled investors with respect to disclosure of its 2014 data breach affecting hundreds of millions of Yahoo! subscribers. The breach, one of the largest in history, compromised Yahoo users' personal information including usernames, passwords, birthdates and telephone numbers.

While the SEC has investigated potential securities law violations related to data breaches since at least 2005, this is the first SEC cybersecurity disclosure enforcement action and follows the release of updated guidance on the topic earlier this year[2]. The SEC's Order Instituting Cease and Desist Proceedings (the "Order")[3] against Altaba tracks the guidance in several ways and demonstrates the SEC's willingness to aggressively pursue violations of disclosure obligations relating to cybersecurity incidents. The guidance focuses on the need to maintain effective disclosure controls and procedures to ensure proper disclosure of material cybersecurity incidents in SEC filings. Specifically, among other items, issuers were reminded of the need to evaluate disclosure in the risk factors and MD&A sections of their SEC filings, including the possibility that significant costs and expenses of a material breach may trigger MD&A disclosure obligations to discuss known trends and uncertainties that may affect liquidity or net revenue. The SEC found Yahoo's filings deficient in both of these areas.

According to the Order, the SEC concluded that Yahoo violated Sections 17(a)(2) and 17(a)(3) of the Securities Act of 1933 and Section 13(a) of the Securities Exchange Act of 1934 (the "Exchange Act"), and certain rules promulgated thereunder, relating to Yahoo's failure to timely disclose the massive data breach discovered in 2014, which the company did not publicly disclose until 2016 when the company was in the process of being acquired by Verizon. Yahoo did not admit or deny the SEC's findings. The SEC's release states that "[a]though information relating to the breach was reported to members of Yahoo's senior management and legal department, Yahoo failed to properly investigate the circumstances of the breach and to adequately consider whether the breach needed to be disclosed to investors."

## AGG Observations

- **The SEC has now shown it will actively pursue enforcement actions relating to a failure to disclose material cybersecurity incidents.** The Yahoo settlement merits scrutiny given its size, scope and related media attention. The SEC, based on its updated guidance and its action against Altaba, is clearly seeking to crack down on perceived cybersecurity breach disclosure deficiencies. All companies, regardless of size and industry, should take heed to conduct a thorough review of their risk management practices, disclosure controls and procedures and insider trading policies in light of the SEC's guidance and enforcement activity.[4]

1 https://www.sec.gov/news/press-release/2018-71
2 https://www.sec.gov/rules/interp/2018/33-10459.pdf
3 https://www.sec.gov/litigation/admin/2018/33-10485.pdf
4 The Yahoo settlement follows the SEC's recent announcement of charges against a former Equifax executive for insider trading in advance of Equifax's announcement of its own devastating data breach in September 2017. See https://www.sec.gov/news/press-release/2018-40.

- **Generic risk factors discussing the potential for data breaches and the likely material consequences of a material breach are not sufficient.** The Order notes that Yahoo's public filings included thorough risk factors outlining the severe negative consequences of a possible breach including "…litigation, remediation costs, increased costs for security measures, loss of revenue, damage to our reputation, and potential liability." Many companies include similar theoretical risk factors in their public filings. In Yahoo's case, however, this type of 'potential breach' language in its SEC filings became problematic, in the SEC's view, once an actual material breach occurred because the language then suggested that a breach was a hypothetical possibility rather than an actual occurrence. The Yahoo action demonstrates the need to reevaluate these disclosures to consider specific disclosure of past material breaches or supplemented disclosure upon the occurrence of an actual breach in the future.

- **Companies should be cognizant of the implications of false or misleading representations made in material agreements filed as exhibits to SEC filings.** The SEC alleges that Yahoo made knowing misrepresentations as to a lack of material data breaches in the acquisition agreement it entered into in connection with the sale of its operating business to Verizon. The acquisition agreement was filed as an exhibit to an 8-K filing in July 2016. The 8-K filing contained typical disclaimers including that representations and warranties contained in the agreement are made solely for the benefit of the parties to the agreement, should not be taken as fact and merely reflect the allocation of risk between the parties[5]. However, despite the disclaimers, the Order cites these knowing misrepresentations contained in the purchase agreement as a factor in its determination that Yahoo violated the securities laws. Companies must now be on alert that the SEC may give additional scrutiny to affirmative representations contained in filed transaction agreements in evaluating compliance with their obligations to make material disclosures to investors.

- **Companies should include outside advisers, including outside counsel and auditors, early in the process when analyzing the disclosure implications of a cybersecurity incident.** The Order specifically notes that "…Yahoo's senior management and legal teams 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." This appears to have been an important factor in the SEC's determination that Yahoo did not have adequate internal disclosure controls in place to properly evaluate the impact of the breach and the need for disclosure in the company's public filings. Determining whether a data breach has occurred and whether notice to potentially affected individuals must or should be provided can be a difficult decision. Public companies also must take into account their obligation to disclose material information to investors in accordance with SEC and stock exchange rules. Involving outside advisors early in the process can help establish a track record of proper procedures in evaluating the implications of a breach and assessing whether an incident is material for purposes of SEC and stock exchange rules.

5 These disclaimers are generally included in response to the SEC's March 2005 Report of Investigation Pursuant to Section 21(a) of the Exchange Act relating to Titan Corporation's filing of a merger agreement containing potentially false or misleading representations regarding Titan's FCPA liability. See https://www.sec.gov/litigation/investreport/34-51238.htm.

## Authors and Contributors

**Brian A. Teras**
Partner, Atlanta Office
404.873.8622
brian.teras@agg.com

**B. Joseph Alley, Jr.**
Partner, Atlanta Office
404.873.8688
joe.alley@agg.com

**Kevin L. Coy**
Partner, DC Office
202.677.4034
kevin.coy@agg.com

not *if*, but *how*.®

## About Arnall Golden Gregory LLP

Arnall Golden Gregory (AGG), an Am Law 200 law firm with 165 attorneys in Atlanta and Washington, DC, takes a "business sensibility" approach when advising clients. AGG provides industry knowledge, attention to detail, transparency and value to help businesses and individuals achieve their definition of success. AGG's transaction, litigation, regulatory and privacy counselors serve clients in healthcare, real estate, litigation, business transactions, fintech, global commerce, government investigations and logistics and transportation. AGG subscribes to the belief "not if, but how.®"
Visit us at www.agg.com.

**Atlanta Office**
171 17th Street, NW
Suite 2100
Atlanta, GA 30363

**Washington, DC Office**
1775 Pennsylvania Avenue, NW
Suite 1000
Washington, DC 20006

To subscribe to future alerts, insights and newsletters: **http://www.agg.com/subscribe/**