PUBLICATION

Public Company Cybersecurity Disclosures: The SEC Means What It Says

Authors: Matthew George White
April 26, 2018

On April 24, 2018, the U.S. Securities and Exchange Commission (SEC) fined Altaba Inc. – formerly known as Yahoo – $35 million for failing to disclose a substantial data breach and cyberattack that occurred in December 2014. This was the first fine issued by the agency alleging that investors were misled by a company's failure to disclose a cyberattack. This action follows closely on the heels of the SEC's interpretive guidance on public company cybersecurity disclosures. We previously analyzed the SEC's guidance and the various considerations a company must evaluate in determining when and if cybersecurity risks and incidents need to be disclosed. Tuesday's action against Altaba makes clear that the SEC is indeed serious about cracking down on public companies' cybersecurity disclosures.

The SEC Order

According to the SEC's order, in late 2014, "Yahoo learned of a massive breach of its user database that resulted in the theft, unauthorized access, and acquisition of hundreds of millions of its users' data, including usernames, birthdates, and telephone numbers." Despite its knowledge of this breach, Yahoo failed to disclose it in its public company filings for nearly two years. Instead, Yahoo claimed in its reports that it only faced the risk of potential future breaches without reporting that an actual data breach had occurred. Yahoo likewise omitted from its risk factor disclosures and management discussion and analysis (MD&A) "known trends or uncertainties with regard to liquidity or net revenue presented by the 2014 data breach."

On or about September 22, 2016, Yahoo finally disclosed the 2014 breach and resulting theft of data by attaching a press release to its Form 8-K. Yahoo also amended its risk factor disclosures and MD&A to reflect the breach. At that time, Yahoo finally corrected prior statements in its 2014 and 2015 Form 10-Ks and Form 10-Qs.

Altaba/Yahoo's Violations

As a result of this conduct, the SEC asserted that Yahoo violated Sections 17(a)(2) and 17(a)(3) of the Securities Act [15 U.S.C. §§ 77q(a)(2) and (3)], which make it unlawful for

any person in the offer or sale of any securities by the use of any means or instruments of transportation or communication in interstate commerce or by use of the mails, directly or indirectly, to obtain money or property by means of any untrue statement of a material fact or any omission to state a material fact necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; or to engage in any transaction, practice, or course of business which operates or would operate as a fraud or deceit upon the purchaser.

The SEC also asserted that Yahoo violated Section 13(a) of the Exchange Act [15 U.S.C. § 78m(a)] and Rules 12b-20, 13a-1, 13a-11, 13a-13, and 13a-15 thereunder [17 C.F.R. §§ 240.12b-20, 240.13a-1, 240.13a-11, 240.13a-13, and 240.13a-15], which require

every issuer of a security registered pursuant to Section 12 of the Exchange Act to file with the Commission, among other things, annual, quarterly, and current reports as the Commission may require, to maintain disclosure controls and procedures designed to ensure that information required to be disclosed by an issuer in

reports it files or submits under the Exchange Act is recorded, processed, summarized, and reported within the time periods specified in the Commission's rules and forms, and mandate that periodic and current reports contain such further material information as may be necessary to make the required statements not misleading.

As noted in Baker Donelson's previous publication, "[c]ompanies should consider the materiality of cybersecurity risks and incidents when preparing disclosures that are required in registration statements under the Securities Act and Exchange Act." Specifically, "[r]eporting of such events can be required when making disclosures through periodic reports such as Forms 10-K and 10-Q, wherein companies must provide timely and ongoing information regarding material cybersecurity risks and incidents that trigger disclosure obligations.

Conclusion and Takeaways

Through this order, the SEC demonstrated its willingness to seek significant fines when public companies fail to heed its warnings to carefully monitor cybersecurity disclosures. However, interestingly enough, the SEC's order did not find any individual company executives liable for the company's conduct. Given the SEC's recent guidance, we may see the SEC being more aggressive with respect to individual executives' conduct in future actions for failing to disclose cyber risks and incidents.

As previously suggested in our prior analysis: "the SEC's focus on cybersecurity-related matters is not going away." Companies need to ensure that they have sufficient policies and procedures in place to address cyber-related concerns, should consider whether any disclosure requirements necessitate disclosure of cyber-related issues, and must evaluate the SEC's guidance when handling and responding to a cyber incident.

If you have any questions regarding these issues or any other cybersecurity or data privacy-related matters, please contact Matthew G. White, CIPP/US, or any member of Baker Donelson's Data Protection, Privacy and Cybersecurity Team.