SEC Brings First Enforcement Action Against a Public Company for Failing to Disclose Data Breach

May 1, 2018 Kit Addleman, Tim Newman

PRACTICES Privacy and Cybersecurity, Litigation

On April 24, 2018, the Securities and Exchange Commission ("SEC" or the "Commission") announced its first enforcement action against a public company for failing to disclose a data breach. In a settled cease-and-desist order, the SEC imposed a $35 million civil penalty against Altaba Inc., formerly known as Yahoo! Inc. ("Yahoo" or the "Company"), based on allegations that the Company violated federal securities laws when it failed to disclose a 2014 data breach affecting more than 500 million user accounts. The Commission has been hinting that enforcement action for disclosure failures was possible since the Division of Corporation Finance first published guidance on the topic in 2011. That guidance was reaffirmed by the Commission earlier this year.

Disclosure Guidance

On October 13, 2011, the SEC's Division of Corporation Finance (the "Division") issued guidance regarding public companies' disclosure obligations related to cybersecurity. In that guidance, the Division highlighted existing disclosure obligations that may be implicated by cyber matters, including risk factors, material litigation, and disclosure controls and procedures.

On February 21, 2018, the SEC Commissioners unanimously approved updated guidance regarding cybersecurity risks. This updated guidance also highlighted existing disclosure obligations potentially implicated by cyber matters, including management's discussion and analysis of financial condition and results of operations ("MD&A") and disclosure controls and procedures.

The SEC's Order Against Yahoo

The SEC's order against Yahoo is the first enforcement action based on a public company's failure to disclose a data breach. According to the SEC, Yahoo learned in late 2014 that its information technology networks and systems had suffered a severe and extensive intrusion by hackers. By December 2014, Yahoo's information security team determined that the personal data of at least 108 million users, including usernames, email addresses, telephone numbers, dates of birth, hashed passwords, and security questions and answers, had been compromised. "Within days," according to the SEC, Yahoo's information security team internally reported the breach to members of the Company's senior management and legal teams. It was later determined that the breach affected more than 500 million Yahoo user accounts.

The SEC alleged that Yahoo's annual reports for FY 2014 and FY 2016, and various quarterly reports in FY 2015 and FY 2016, contained false and misleading statements. According to the SEC's allegations, Yahoo disclosed only the potential risks associated with cybersecurity matters and, despite knowing that the Company had already discovered a data breach, failed to disclose the actual breach.

The SEC also alleged that Yahoo affirmatively represented to Verizon, another public company that had entered into negotiations with Yahoo for its purchase, that it was only aware of four minor data breaches that Yahoo had suffered. These false representations were made publicly available in a Form 8-K, which Yahoo filed with the Commission on July 25, 2016 while the Verizon acquisition was pending.

Finally, the SEC asserted that Company management failed to establish or implement the necessary internal controls to "assess the scope, business impact, or legal implications of the breach, including how and where the breach should have been disclosed." The Company also allegedly failed to determine whether the breach "rendered, or would render, any statements made by Yahoo in its public filings misleading."

Yahoo acknowledged the internal controls shortcomings in its Form 10-K for FY 2016 filed in March 2017 when the Company disclosed that certain senior executives failed to act sufficiently upon the information discovered by the Company's information security team. The Company attributed its lack of prior disclosure of the breach to failures in communication, management, inquiry, and internal reporting.

Based on these failures, the SEC alleged that Yahoo violated Sections 17(a)(2) and 17(a)(3) of the Securities Act, which prohibit public companies from making untrue statements or omissions in the sale of securities and from engaging in practices that operate as a fraud upon investors. The SEC also charged Yahoo with violations of Section 13(a) of the Exchange Act and corresponding Commission rules which require every issuer to file periodic reports, maintain disclosure controls, and ensure that such reports are not misleading. Yahoo agreed to a cease-and-desist order, a $35 million civil penalty and to cooperate with any additional Commission investigations or litigation that may result from Yahoo's failure to disclose.

Takeaways

With guidance regarding disclosure of cybersecurity risks and breaches first published in 2011 and updated guidance published earlier this year to emphasize the seriousness with which the SEC considers cybersecurity concerns, this enforcement action is no surprise. As the first enforcement action of its kind, the enforcement staff appears to have selected Yahoo because the facts, as recited in the Order, echo concerns highlighted in the 2011 and 2018 guidance. The SEC's Order against Yahoo cites the severity of the breach, the amount of time that passed before it was disclosed, the number of allegedly misleading disclosures, and Yahoo's statements in its FY 2016, Form 10-K acknowledging that the "relevant legal team had sufficient information to warrant substantial further inquiry in 2014, and they did not sufficiently pursue it." Steven Peikin, Co-Director of the SEC Enforcement Division, noted that the SEC has cautioned that a company's disclosure in response to a cyber incident "could be so lacking that an enforcement action would be warranted" and stated that the Yahoo facts were "clearly such a case."

We can expect the SEC will remain focused on cybersecurity disclosures, and with this new precedent in hand, we will likely see the Commission bringing more cases. In light of this order, public companies should review their disclosure controls and procedures. Attention should be given to identifying for the disclosure committee, senior officers, and directors all cybersecurity matters, including breach attempts and incidents, for a discussion of ongoing disclosure obligations and appropriate updates to controls processes.

View the order.