Derek Kearl

Partner
801.799.5857
Salt Lake City
jdkearl@hollandhart.com

SEC Issues First Ever Enforcement Action For Failure to Disclose a Data Breach, Obtaining $35 Million Penalty

Publication — 05/18/2018

The U.S. Securities and Exchange Commission announced on April 24, 2018 that Yahoo! (now known as Altaba, Inc.) agreed to pay a $35 million civil penalty to resolve claims that it failed to appropriately and timely disclose the 2014 data breach of involving hundreds of millions of its user accounts. This marks the first enforcement action and fine the SEC has sought based on allegations that a company misled investors by failing to disclose a cybersecurity attack. It also comes in the wake of the SEC's long-awaited guidance on cybersecurity disclosures for public companies, issued in February 2018, as discussed in a previous client alert.

The enforcement action highlights the critical importance of following that guidance, including developing comprehensive, enterprise-wide policies and procedures to ensure that cybersecurity risks and incidents are timely reported up the corporate ladder and appropriately disclosed.

The Data Breach

According to its cease-and-desist Order, the Commission found that, in December 2014, Yahoo's information security team discovered a massive breach of its user database that resulted in the theft, unauthorized access, or acquisition of hundreds of millions of its users' personal data. Hackers associated with the Russian Federation stole copies of Yahoo's user database files containing the personal data of at least 108 million users. The personal data in the stolen files included highly sensitive information Yahoo's information security referred to as Yahoo!'s “crown jewels”: usernames and passwords, dates of birth, telephone numbers, and answers to security questions.

Within days of the information security team reaching these conclusions, Yahoo's Chief Information Security Officer notified members of Yahoo!'s senior management and legal teams of the breach.

Yahoo's Disclosure Response

In spite its knowledge of the 2014 data breach, according to the SEC's Order, Yahoo did not disclose the data breach in its public filings for nearly two years. Instead, Yahoo's risk factor disclosures in its annual and quarterly reports from 2014 to 2016 claimed the company faced the risk of potential future data breaches that might expose the company to loss of its users' personal information stored on its information systems, without disclosing that a massive data breach had, in fact, already occurred. Management's discussion and analysis of financial condition and result of operations (“MD&A”) in those reports did not identify known trends or

uncertainties regarding liquidity or net revenue presented by the 2014 data breach. As a result, the SEC determined Yahoo's disclosures to be materially misleading in violation of federal securities laws.

It was not until September 22, 2016 that Yahoo disclosed the 2014 breach and the resulting theft of data involving 500 million of its user accounts. The company later acknowledged that its “relevant legal team had sufficient information to warrant substantial further inquiry in 2014, and they did not sufficiently pursue it.” The SEC's Order states that senior management and relevant legal staff did not properly assess the scope, business impact, or legal implications of the breach, including how 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.

The SEC's Order is critical of senior management and legal teams for not sharing information regarding the breach with Yahoo's auditors and outside counsel in Order to assess the company's disclosure obligations in its public filings. The Commission found that Yahoo did not maintain disclosure controls and procedures sufficient to ensure that reports from Yahoo's information security team raising actual or threatened incidents of theft of user data were properly and timely assessed to determine how and where the breaches should be disclosed in Yahoo's public filings.

The SEC Order is also critical of Yahoo's disclosure omissions in connection with the sale of its operating business to Verizon in July 2016. The Commission found that, during negotiations, Yahoo falsely represented to Verizon that it was only aware of a few minor breaches involving users personal information, but did not disclose the 2014 theft of hundreds of millions of user data. After disclosure of the breach, Yahoo and Verizon renegotiated the terms of the sale of Yahoo's operating business, including a reduction in the acquisition price of $350 million, a 7.25% discount.

Violations of Federal Securities Laws and Penalty

As a result of Yahoo's disclosure deficiencies identified in the Order, the SEC found that Yahoo violated Sections 17(a)(2) and 17(a)(3) of the Securities Act, Section 13(a) of the Exchange Act (and its implementing regulations). As a result of a settlement reached with Yahoo, the SEC Ordered Yahoo to pay a civil money penalty of $35 million and to cease and desist from any future violations of federal securities laws. Yahoo is also required under the Order to continue to fully cooperate with the SEC in its ongoing investigation of the matters described in the Order, including the continued production of documents without subpoena, and making company directors and officers available to provide interviews and testimony.

Lessons Learned

The Order is emblematic of the SEC's enhanced focus on cybersecurity issues in the face of increasingly frequent, material cybersecurity attacks, and emphasizes that public companies must carefully scrutinize their

cybersecurity and data breach controls and procedures so that data breaches are appropriately and timely disclosed. In the case of Yahoo, the SEC found a severe failure in the company's evaluation of the data breach and its disclosure to investors. Indeed, in the press release accompanying the Order, the SEC stated: “We do not second-guess good faith exercises of judgment about cyber-incident disclosure. But we have also cautioned that a company's response to such an event could be so lacking that an enforcement action would be warranted. This is clearly such a case.”

The Order also highlights the need for companies to measure their controls and procedures against SEC's interpretive guidance. Companies would be well-served to adhere to that guidance, including establishing comprehensive controls and procedures that enable them to identify and evaluate the significance of cybersecurity risks and incidents, assess and analyze their impact on a company's business, provide for open communications between technical experts and senior management, and make timely and appropriate disclosures regarding such risks and incidents. For companies who do not, the Order serves as a cautionary tale.