May 3, 2018

Yahoo! Agrees to $35 Million SEC Penalty for Failure to Disclose Cyber Incident

On April 24, 2018, the Securities and Exchange Commission announced that Altaba, the company formerly known as Yahoo! Inc., agreed to pay a $35 million penalty as part of a cease-and-desist order to settle charges that it misled investors by failing to disclose a significant data breach in which hackers stole personal data relating to hundreds of millions of Yahoo! accounts in 2014. This was the first fine issued by the SEC based on allegations that investors were misled by a company's failure to disclose a cyberattack and highlights the SEC's increasing focus on cybersecurity issues and related disclosure obligations for public companies.

The settlement comes two months after the SEC's release of guidance to assist public companies in preparing disclosures concerning cybersecurity risks and incidents. The guidance, discussed in a prior client alert, noted that cybersecurity risk management policies and procedures are key elements of enterprise-wide risk management, including as it relates to compliance with the federal securities laws. Registrants were reminded to assess whether they have sufficient disclosure controls and procedures in place to ensure that relevant information about cybersecurity risks and incidents is processed and reported to the appropriate personnel, including up the corporate ladder, to enable senior management to make disclosure decisions and certifications.

Background

According to the findings in the SEC's order (which Yahoo! has neither admitted nor denied), in late 2014, Yahoo!'s internal information security team learned of a large-scale breach of its user database that resulted in the theft, unauthorized access, and acquisition of hundreds of millions of its users' data. By December 2014, Yahoo!'s information security team, including its Chief Information Security Officer, had determined that the hackers had stolen copies of Yahoo!'s user database files containing the personal data of at least 108 million users, and likely Yahoo!'s entire user database of billions of users. The personal data in the stolen files included highly sensitive information that Yahoo!'s information security team referred to as Yahoo!'s "crown jewels": Yahoo! usernames, email addresses, telephone numbers, dates of birth, passwords, and security questions and answers.

Within days after Yahoo!'s information security team reached these conclusions, members of Yahoo!'s senior management and internal legal teams were notified.

Disclosure Response

Although Yahoo! was aware of the data breach in 2014, it did not disclose the data breach in its public filings for nearly two years. Yahoo!'s risk factor disclosures in its annual and quarterly reports for 2014 through 2016 advised that the company faced the risk of data breaches that might expose the company to loss of its users' personal information stored in its information systems, but did not disclose that a large data breach had in fact already occurred. The management's discussion and analysis of financial condition and results of operations in those reports did not identify known trends or uncertainties with regard to liquidity or net revenue presented by the 2014 data breach. According to the SEC, these disclosures were therefore materially misleading.

As later acknowledged in Yahoo!'s Form 10-K for fiscal year 2016, the company's "relevant legal team had sufficient information to warrant substantial further inquiry in 2014, and they did not sufficiently pursue it." According to the SEC's order, Yahoo! senior management and relevant legal staff 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.

In addition, the order 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. The SEC found that Yahoo! did not maintain 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.

Moreover, as described in the order, Yahoo!'s disclosure omissions continued in connection with the proposed sale of its operating business to Verizon Communications, Inc. in July 2016. Although Yahoo! was aware of additional evidence in the first half of 2016 indicating that its user database had been stolen, Yahoo! made affirmative representations denying the existence of any significant data breaches in a July 2016 stock purchase agreement with Verizon, by which Verizon was to acquire Yahoo!'s operating business for $4.825 billion. The stock purchase agreement was attached to a Form 8-K filed subsequently with the SEC. After disclosure of the breach, and after renegotiation of the terms of the sale of Yahoo!'s operating business, Verizon and Yahoo! agreed to a reduction in the acquisition price for Yahoo!'s operating business of $350 million, representing a 7.25% discount.

As a result of the disclosure deficiencies identified in the settlement, the SEC found that Yahoo! violated Sections 17(a)(2) and 17(a)(3) of the Securities Act of 1933 and Section 13(a) (and implementing regulations) of the Securities Exchange Act of 1934, and imposed a civil money penalty of $35 million.

Implications for Public Companies

The SEC has repeatedly signaled its enhanced focus on cybersecurity issues given the increase in frequency and scope of cyberattacks, and emphasized that companies should scrutinize their disclosure, controls and procedures as they relate to cybersecurity issues. In connection with the 2018 interpretive release regarding disclosure of cybersecurity incidents, SEC Chairman Jay Clayton stated: "I urge public companies to examine their controls and procedures, with not only their securities law disclosure obligations in mind, but also reputational considerations around sales of securities by executives." More recently, Division of Corporation Finance Director William Hinman, during his April 26 testimony before the Capital Markets, Securities and Investment Subcommittee of the U.S. House Committee on Financial Services stated that when his staff sees news reports that a hack has occurred, they call the company's counsel and ask to be walked through the analysis of why a particular breach was not material.

When a company is aware that it has been the victim of a significant cyberattack, merely disclosing the risk of such an attack can be misleading. The SEC has regularly cautioned registrants that risk factor disclosures that are stated in the hypothetical, when in fact the risk has come to pass, is misleading. Notably, in the press release accompanying the order, the SEC noted that "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 SEC also emphasized that public companies should have controls and procedures in place to properly evaluate cyber incidents and disclose material information to investors.

There remains no bright line standard as to when a cybersecurity incident triggers a public company's disclosure obligations; however, the SEC's order makes clear that a company with ineffective disclosure controls and procedures as they relate to cybersecurity incidents may find it difficult to persuade the SEC of the adequacy of its cybersecurity disclosures. Controls and procedures should enable registrants to identify cybersecurity risks and incidents, assess and analyze their impact on a registrant's business, evaluate the significance of such risks and incidents, provide for open communications between technical experts and disclosure advisers, and make timely disclosures regarding such risks and incidents. The SEC has also emphasized that registrants should consider whether they need to revisit or refresh previous disclosure during the process of investigating a cybersecurity incident.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

Mark S. Bergman
+44-20-7367-1601
mbergman@paulweiss.com

Roberto J. Gonzalez
+1-202-223-7316
rgonzalez@paulweiss.com

David S. Huntington
+1-212-373-3124
dhuntington@paulweiss.com

Richard C. Tarlowe
+1-212-373-3035
rtarlowe@paulweiss.com

Hank Michael
+1-212-373-3892
hmichael@paulweiss.com