ROPES & GRAY ALERT

Securities & Public Companies ▪ Privacy & Cybersecurity

May 4, 2018

$35 Million Yahoo Fine Reflects SEC's Heightened Cybersecurity Focus

On April 24, 2018, the Securities and Exchange Commission ("SEC") announced the settlement of its first-ever enforcement action against a company for an alleged failure to disclose a cybersecurity breach. Altaba Inc., the company formerly known as Yahoo! Inc. ("Yahoo"), agreed to pay $35 million to settle charges that it misled investors by not disclosing one of the world's largest data breaches involving hundreds of millions of user accounts. This settlement underscores the agency's increasing focus on cybersecurity and the importance it places on disclosures about cyber incidents.

In December 2014, hackers allegedly stole what Yahoo called its "crown jewels" – user names, email addresses, phone numbers, birthdates, hashed passwords, and security questions and answers – for more than 500 million accounts. It was the "largest known theft of user data" at the time, according to the SEC's order. Within days, Yahoo's information security team allegedly became aware of the intrusion and informed Yahoo's senior management and internal legal teams.

Yahoo did not publicly disclose the breach until two years later. The SEC claims that Yahoo "materially misled" investors throughout this period by stating that the company faced a risk of potential data breaches without mentioning that a massive data breach had already occurred and by omitting known effects of the breach in its management discussion and analysis ("MD&A"). According to the SEC, Yahoo did not share the existence of the breach with its auditors or outside counsel. Further, the SEC alleges that Yahoo had falsely represented that it had no data breaches in its stock purchase agreement with Verizon Communications Inc. (which Yahoo publicly filed as an Exhibit to its Current Report on Form 8-K).[1] When Yahoo ultimately disclosed the breach in September 2016, its market capitalization fell by almost $1.3 billion, and Verizon renegotiated the stock purchase agreement to reduce the purchase price for Yahoo's operating business by 7.25 percent.

The SEC alleges that Yahoo's failure to disclose the breach violated Sections 17(a)(2) and 17(a)(3) of the Securities Act, and that Yahoo's disclosure failure and failure to maintain disclosure controls and procedures violated Section 13(a) of the Exchange Act and Rules 12b-20, 13a-1, 13a-11, 13a-13, and 13a-15. In addition to the $35 million fine, the settlement agreement requires Yahoo to cease and desist from committing any further violations of these laws. The SEC has stated that its investigation is still continuing, and thus it is possible there could be actions against company representatives in their individual capacities. Yahoo also faces an $80 million settlement payment to end a shareholder suit based on similar allegations, which is pending court approval.

The SEC's settlement order comes on the heels of its February 21, 2018 Commission Statement and Guidance on Public Company Cybersecurity Disclosures, which emphasized the SEC's view that companies are obligated to disclose material cybersecurity risks and incidents. The 2018 guidance recognized that "a company may require time to discern the implications of a cybersecurity incident" but warned that "an ongoing internal or external investigation – which often can be lengthy – would not on its own provide a basis for avoiding disclosures of a material cybersecurity incident." The 2018 guidance also encouraged companies to adopt disclosure controls and procedures

[1] It is unclear whether schedules to the agreement disclosed any data breaches, but the schedules were not filed in connection with the Form 8-K.

related to cybersecurity incidents, and to assess their compliance regularly. The 2018 guidance expanded upon 2011 guidance issued by the staff of the Division of Corporation Finance.

The SEC's heightened focus on public company cybersecurity disclosures reflects its increasing activity in the cybersecurity realm. In a Statement on Cybersecurity issued September 20, 2017, SEC Chairman Jay Clayton promised the agency would "prioritize its efforts to promote effective cybersecurity practices." Five days later, the Division of Enforcement launched a Cyber Unit to target cyber misconduct, including the failure of public companies to disclose cyber risks and incidents, and the failure of registered entities to appropriately safeguard information. The SEC has repeatedly brought actions against registered entities for allegedly failing to implement reasonable data security policies and procedures. And year after year, the SEC's Office of Compliance Inspections and Examinations has named cybersecurity one of its five examination priorities.

In short, it does not appear that the SEC is losing interest in the "cyber threat" – the "greatest threat to our markets right now," according to Division of Enforcement co-director Steven Peikin. While the scope of the SEC's enforcement authority in this space has not yet been tested, these developments do highlight steps that companies can take to mitigate the risk of becoming the target of an SEC investigation in the first place. In particular, the Yahoo settlement highlighted that companies can reduce exposure to SEC cybersecurity enforcement by evaluating and, where appropriate, enhancing their disclosure controls and procedures related to cybersecurity risks and incidents. Ropes & Gray has previously outlined important considerations for cybersecurity disclosures in an Alert available here.

In finding that the representations included in the agreement with Verizon constituted public disclosure of the absence of a cyber breach, the order is a reminder that the SEC continues to take the position it did in the 2005 Titan 21(a) report that statements made in agreements that are filed with the Commission are not private contractual matters but constitute disclosures upon which investors may rely.[2]

For more information on the Yahoo settlement or to discuss data security or securities issues generally, please contact a member of our securities & public companies or privacy & cybersecurity practice groups.

[2] Note that the SEC's finding comes despite the inclusion by Yahoo of so-called "Titan disclaimers" in Yahoo's Form 8-K, which stated, among other things, the transaction agreements that were attached as exhibits to the Form 8-K were intended to provide stockholders with information regarding their terms, but were not intended to provide any other factual information about Yahoo, and that stockholders should not rely on the representations, warranties and covenants contained in the transaction agreements as characterizations of the actual state of facts or condition of Yahoo or Verizon.