DORSEY
DORSEY + WHITNEY LLP

Failure to Disclose Leads to $35 Million Penalty in the Yahoo! Cybersecurity Breach

April 26, 2018 – Governance & Compliance Insider
by Cam C. Hoang

The Securities and Exchange Commission (the "SEC") announced Tuesday that Altaba, the entity formerly known as Yahoo! Inc., has agreed to pay a $35 million penalty to settle charges that it misled investors by failing to disclose one of the world's largest data breaches in which hackers stole personal data relating to hundreds of millions of user accounts.

According to the SEC's order, within days of the December 2014 intrusion, Yahoo's information security team learned that Russian hackers had stolen what the security team referred to internally as the company's "crown jewels": usernames, email addresses, phone numbers, birthdates, encrypted passwords, and security questions and answers for hundreds of millions of user accounts. Although information relating to the breach was reported to members of Yahoo's senior management and legal department, Yahoo failed to properly investigate the circumstances of the breach and to adequately consider whether the breach needed to be disclosed to investors. The fact of the breach was not disclosed to the investing public until more than two years later, when in 2016 Yahoo was in the process of closing the acquisition of its operating business by Verizon Communications, Inc.

In the order, the SEC finds that Yahoo's post-breach disclosure in quarterly and annual reports was too general, stating that the company faced only the risk of, and negative effects that might flow from, data breaches. The company failed to disclose the actual breach or its potential business impact and legal implications.

In addition to deficiencies in Yahoo's disclosure to investors, the SEC's order found that Yahoo did not share information regarding the breach with its auditors or outside counsel in order to assess the company's disclosure obligations in its public filings.

Finally, the SEC's order found that Yahoo failed to maintain disclosure controls and procedures designed to ensure that reports from Yahoo's information security team concerning cyber breaches, or the risk of such breaches, were properly and timely

Related People

- Cam C. Hoang

Related Capabilities

- Corporate Governance & Compliance
- Mergers & Acquisitions
- Government Enforcement & Corporate Investigations

assessed for potential disclosure.

In its Statement and Guidance on Public Company Cybersecurity Disclosures, released earlier this year, the SEC reiterates that public companies are required to disclose material risks and incidents, including those related to cybersecurity, in their current and periodic reports. The SEC encourages companies to continue to use current reports to disclose material cybersecurity-related information promptly as this practice reduces the risk of selective disclosure. Furthermore, beyond requirements explicitly found in SEC regulations, companies are also required to disclose material information and revisit previous disclosure, especially during a cybersecurity investigation, as may be necessary to ensure the company's filings are not misleading. Notably, perhaps in recognition of how rapidly the scope of a breach may evolve, the SEC provides that companies "have a duty to correct prior disclosures that the company determines were untrue at the time it was made, or a duty to update a disclosure that becomes materially inaccurate after it is made." See our earlier memo for a summary of the SEC's guidance.

In evaluating the range of potential disclosure for quarterly and annual reports, companies should consider that cybersecurity breaches or the risk of such breaches may trigger disclosure in the Management's Discussion and Analysis, if the breach presents a material event, trend or uncertainty that has had or is reasonably likely to have a material effect on results of operations, liquidity or financial condition. Furthermore, financial statements may need to reflect costs incurred, insurance proceeds and contingent liabilities resulting from claims. A cybersecurity breach may also need to be addressed in the description of business, discussion of legal proceedings and effectiveness of internal controls and disclosure controls and procedures.

Even before the next quarterly or annual report, companies should consider whether the information available on the cybersecurity breach is material and should be communicated to investors in a current report in order to reduce the risk of selective disclosure in violation of Regulation FD. If material information on a cybersecurity breach is not publicly disclosed in a current report, companies should consider whether it is appropriate to impose an event-specific blackout on trading in the company's stock, in accordance with applicable insider trading policies. Determining the population of employees and other individuals who know, or in hindsight should have known, about the breach, and who should be subject to the event-specific blackout, deserves careful consideration, as demonstrated by the Equifax experience, where high-ranking executives traded in the company's stock after a cybersecurity breach was discovered but before it was announced.