JONES DAY

COMMENTARY

MAY 2018

SEC Announces Yahoo Will Pay $35 Million for Failure to Disclose Data Security Incident

IN SHORT

The Situation: The SEC accused Altaba Inc., then known as Yahoo! Inc., of misleading investors by failing to disclose a major data breach orchestrated by Russian hackers.

The Result: Altaba has agreed to pay $35 million to settle the allegations.

Looking Ahead: The events indicate that SEC enforcement activity is yet another potential consequence faced by companies for not properly disclosing a data security incident.

The U.S. Securities and Exchange Commission ("SEC") announced a cease-and-desist order in which Altaba Inc., formerly known as Yahoo! Inc., agreed to pay $35 million to settle allegations it misled investors by failing to disclose for nearly two years "one of the world's largest data breaches." According to the SEC, Yahoo learned in December 2014 that Russian hackers had acquired usernames, email addresses, phone numbers, birthdates, encrypted passwords, and security questions and answers for hundreds of millions of user accounts. The SEC noted Yahoo's periodic disclosures regarding cybersecurity risk misleadingly claimed the company faced only the risk of potential future data breaches without disclosing a massive data breach had in fact already occurred. The SEC focused on the apparent lack of controls and procedures to assess cyber-disclosure obligations, leaving investors unaware of the massive data breach.

> The SEC clearly intends for Yahoo's $35 million penalty to cause companies to implement data security incident responses and disclosure protocols not only for consumers but also for investors.

Prior SEC Guidance Regarding Disclosure of Data Security Incidents

In October 2011, the SEC's Division of Corporation Finance issued guidance regarding its views of disclosure obligations for cybersecurity risks and data security incidents. Yahoo's $35 million penalty—the first of its kind imposed on a publicly traded company for failure to disclose a data security incident—comes in the wake of more recent guidance from the SEC. In February 2018, the SEC announced that public companies were required to implement comprehensive disclosure protocols and procedures that would allow them to make accurate and timely disclosure of material cybersecurity risks and incidents. The SEC also stated that companies were required to report cybersecurity risks under existing federal securities reporting laws, including in quarterly and annual reports. Companies were specifically advised to evaluate the materiality of cybersecurity risk by examining prior data security incidents, probability of recurrence, adequacy of preventative actions, additional protection costs, and potential for reputational harm.

Key Takeaways from the Yahoo Penalty

The SEC clearly intends for Yahoo's $35 million penalty to cause companies to implement data security incident responses and disclosure protocols not only for consumers but also for investors. The cease-and-desist order specifically faulted Yahoo for failing to have such procedures in place. It also faulted Yahoo for disclosing only that it faced the risk of potential future data breaches without disclosing the massive cybersecurity breach that had already occurred. Clearly for any issuer, as with other statements in SEC filings, the information disclosed should be accurate.

The SEC has not provided specific guidance on what circumstances would justify SEC sanctions in the future, but they have stated they will not second-guess good-faith exercises of judgment about cyber-incident disclosure. One practical takeaway from this matter is that issuers should promptly investigate such incidents and make a reasoned decision regarding disclosure from a securities law perspective. The challenge may be when a breach must be disclosed to consumers, individuals, or customers under data breach notification laws and/or contracts, but would not be material from a securities law disclosure perspective. It may be a best practice to document such a decision to be prepared to explain the analysis supporting the decision in case of future inquiries or litigation.

This penalty can only be viewed as intending to focus the issuer community and give teeth to the SEC's prior guidance. We also note the SEC has said its investigation is continuing, which is generally a signal they are still considering an action against individuals. The risk of SEC enforcement now joins the litany of other potentially significant consequences of failing to disclose a data security incident: class action

suits, federal securities fraud litigation, congressional inquiries, and government investigations by data protection authorities, including the FTC, state attorneys general, and industry-specific regulators.

THREE KEY TAKEAWAYS

1. The SEC faulted Yahoo for disclosing only that it faced the risk of potential future data breaches and not disclosing the massive breach that had already occurred.
2. While the SEC has not provided specific guidance regarding what circumstances would justify sanctions in the future, it has stated good-faith exercises of judgment about cyber-incident disclosure will not be second-guessed.
3. Companies should promptly investigate data breach incidents and, from a securities law perspective, make a reasoned decision regarding disclosure.


Michael J. McConnell
Atlanta


Joan E. McKown
Washington


Lisa M. Ropple
Boston


Samir C. Jain
Washington

Christopher Hurld, *Jay Johnson*, *James T. Kitchen*, *Andrew M. Ellis*, and *Mary A. Myers* *assisted in the preparation of this* Commentary.

All Contacts >>>

YOU MIGHT BE INTERESTED IN: **Go To All Recommendations >>**

Supreme Court Rules on State Court Jurisdiction over Securities Act Lawsuits

SEC Releases Guidance on Public Company Cybersecurity Disclosures

Ninth Circuit Finds Data Breach Customers Have Initial Standing to Sue

---

SUBSCRIBE SUBSCRIBE TO RSS
