# With $35 Million Fine, SEC Shows Late Cyberbreach Disclosure Can Result in Enforcement

April 26, 2018

## Yahoo! Order Is SEC's First Cyber-Disclosure Enforcement Action

On April 24, the Securities and Exchange Commission charged Altaba Inc., formerly Yahoo! Inc., with misleading shareholders by waiting almost two years to disclose its 2014 data breach. Consenting to a **cease-and-desist order**, Altaba agreed to pay a $35 million penalty in the first SEC enforcement action against a public company relating to cyberbreach notification. The SEC's action follows a trend by **state attorneys general** and **other regulators** in exacting significant penalties from companies that fail to provide timely breach notification. Yahoo! previously reached an $80 million settlement to resolve a class-action securities case for failure to disclose the breach, and currently faces a class-action lawsuit by users who claim their information was stolen.

The SEC's order provides helpful insight into when it will view a company's cybersecurity disclosures as warranting enforcement action.

### Yahoo!'s 2014 Cyberbreach

In 2014, Yahoo! learned of a large-scale breach of its user database that resulted in the theft of hundreds of millions of customer usernames, encrypted passwords, security questions and answers, birthdates and telephone numbers. Yahoo!'s internal information-security team quickly became aware of the hack, and by December 2014, had characterized what was stolen as its "crown jewels." Within days of reaching this determination, members of Yahoo!'s senior management and legal teams received internal reports from Yahoo!'s chief information security officer regarding the theft.

### Delayed Disclosure to Auditors, Outside Counsel and the Public

According to the SEC, despite being aware of the breach, Yahoo! senior management and 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." Moreover, Yahoo!'s senior management and legal teams did not share information regarding the breach with Yahoo!'s auditors or outside counsel, and, according to the SEC, Yahoo! did not have proper procedures in place to assess and elevate information about theft of user data, including how and where such breaches should be disclosed in Yahoo!'s public filings.

Yahoo! eventually disclosed the incident in September 2016, shortly before it closed the sale of its operating unit to Verizon Communications Inc. The day after the disclosure, Yahoo!'s market capitalization fell by nearly $1.3 billion—a 3% decrease. Yahoo! and Verizon thereafter agreed to a 7.25% reduction in the acquisition price for Yahoo!'s operating business. Prior to publicly acknowledging the breach, Yahoo! disclosed in its annual and quarterly reports for 2014-2016 only that it "faced the risk of data breaches and any negative effects that might flow from future breaches," not the 2014 breach itself. In addition, Yahoo! affirmatively represented to Verizon in the purchase and sale agreement, which was included in a July 2016 public filing, that it was "unaware of any security breaches with a 'Business Material Adverse Effect.'"

### What This Means Going Forward

With the Yahoo! order, the SEC is clearly signaling that when a company is aware of a major successful cyberattack, merely disclosing the *risk* of such an attack can be misleading. At the same time, the Yahoo! order also indicates that the SEC does not expect immediate disclosure of a cyberattack. The SEC did not conclude that Yahoo! should have disclosed the breach in a Form 8-K upon becoming aware of it. Instead, the SEC indicated that the breach should have been disclosed over the following two years in its regular periodic reports. This is consistent with the **Commission Statement and Guidance on Public Company Cybersecurity Disclosures**, which recognized that "a company may require time to discern the implications of a cybersecurity incident," but also noted that "an ongoing or external investigation—which can often be lengthy—would not on its own provide a basis for avoiding disclosures of a material cybersecurity incident."

In a press release accompanying the Yahoo! order, the SEC contrasted two different kinds of breach disclosure cases: "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." One of the reasons the Yahoo! case fell into the latter category is its lack of adequate and effective data breach disclosure protocols. As the press release further noted: "Yahoo!'s failure to have controls and procedures in place to assess its cyber-disclosure obligations ended up leaving its investors totally in the dark about a massive data breach. Public companies should have controls and procedures in place to properly evaluate cyber incidents and disclose material information to investors."

The potential remains for the SEC to pursue charges against individual officers of a public company that fails to make adequate and timely disclosures concerning data breach risks and incidents. The investigation into Yahoo!'s disclosures remains ongoing, and we will provide updates on our **Cyber Blog** of any important developments.

One final point – the SEC's emphasis on a representation made by Yahoo! in the Verizon purchase and sale agreement is a reminder that the SEC believes that investors rely on these statements, when included in SEC filings, as if they were intended as disclosures instead of risk-allocation devices, as parties to M&A agreements often assume. The SEC previously addressed this in the 2005 **Titan 21(a) report**, and appears to be focusing on it again.

---

If you have any questions regarding the matters covered in this publication, please contact any of the lawyers listed below or your regular Davis Polk contact.


| | | |
|---|---|---|
| **Avi Gesser** | **212 450 4181** | **avi.gesser@davispolk.com** |
| **Joseph A. Hall** | **212 450 4565** | **joseph.hall@davispolk.com** |
| **Sophia Hudson** | **212 450 4762** | **sophia.hudson@davispolk.com** |
| **Lawrence Portnoy** | **212 450 4874** | **lawrence.portnoy@davispolk.com** |
| **David J. Robles** | **212 450 3088** | **david.robles@davispolk.com** |
| **Sarah K. Solum** | **650 752 2011** | **sarah.solum@davispolk.com** |
| **Linda Chatman Thomsen** | **202 962 7125** | **linda.thomsen@davispolk.com** |
| **Richard D. Truesdell, Jr.** | **212 450 4674** | **richard.truesdell@davispolk.com** |