**Client Alert** | US Public Company Advisory / Data, Privacy & Cybersecurity

# SEC Fines Yahoo $35 Million for Failure to Timely Disclose a Cyber Breach

**April 2018**

**Authors:** Steven R. Chabinsky, Michelle Rutta, Colin Diamond, Dov M. Gottlieb, Irina Yevmenenko

On April 24, 2018, the Securities and Exchange Commission (the "SEC") announced that Altaba Inc. f/d/b/a Yahoo! Inc. ("Yahoo") agreed to pay a $35 million penalty to settle charges that it misled investors by failing to disclose a 2014 personal data breach impacting more than 500 million user accounts.[1] This is the SEC's first enforcement action for failure to make timely disclosure regarding cybersecurity risks or cyber incidents. The proceeding follows the SEC's recent release of updated cybersecurity disclosure guidance for reporting companies (the "New Guidance")[2] and reinforces the fact that the agency is focused on companies' cybersecurity disclosure practices.

According to the SEC's settlement order[3] (the "Order"), Yahoo not only suspected by late 2014, but in fact concluded by then, that hackers stole the personal data of at least 108 million of its users, and potentially the entire multi-billion user database. Internally, Yahoo's information security team considered this data to be the company's "crown jewels." Yet Yahoo took nearly two years to disclose the breach and its potential business impact and legal implications. In addition to this material omission, the SEC found that Yahoo made material misstatements in its public filings from 2014 through mid-2016. Ultimately, the public learned of the breach in September 2016, by way of a press release that the company attached as an exhibit to a Form 8-K. At the time, Yahoo was in the process of closing the acquisition of its core internet operating business by Verizon Communications Inc.[4] As a clear sign of the materiality of the breach, investors punished the company's stock the very next day with a 3 percent loss, representing $1.3 billion in market capitalization. In addition, the disclosure led to a renegotiation of the acquisition agreement, resulting in a 7.25 percent reduction in purchase price.

---

1 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 law suit by users who claim their information was stolen. In October of 2017, after its purchase by Verizon, Yahoo announced that a post-transaction forensic investigation revealed that hackers made their way to all 3 billion user accounts as early as 2013.

2 The New Guidance is available here. For detailed information on the SEC's new cybersecurity guidance, see our prior alert, "SEC Issues Interpretive Guidance on Public Company Cybersecurity Disclosures: Greater Engagement Required of Officers and Directors".

3 The SEC's Order is available here.

4 Verizon ultimately acquired Yahoo's internet operating business in June 2017 and Yahoo subsequently changed its name to Altaba Inc.

With respect to these misstatements and omissions, the SEC determined that Yahoo violated a number of provisions of the Securities Act of 1933 (the "Securities Act") and the Securities Exchange Act of 1934 (the "Exchange Act"), as well as related rules.[5] Specifically, the Order found that:

- Yahoo's risk factor disclosures in its annual and quarterly reports from 2014 through 2016 were materially misleading in that they claimed the company only faced the "risk of potential future data breaches" that might expose the company to loss and liability "without disclosing that a massive data breach had in fact already occurred.";
- Yahoo's Management's Discussion and Analysis of Financial Condition and Results of Operations ("MD&A") in those reports was materially misleading to the extent it omitted known trends or uncertainties with regard to liquidity or net revenue presented by 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";
- Yahoo did not inform its own auditors or outside counsel about the breach so they could assess the company's disclosure obligations in its public filings; and
- 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 assessed for potential disclosure obligations.

The Order also found disclosure violations in connection with the proposed sale of the company's operating business in July 2016, determining that 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 23, 2016 stock purchase agreement [that] was attached to a Form 8-K filed with the [SEC] on July 25, 2016."

In addition to the monetary settlement, without admitting or denying the SEC's allegations, Yahoo agreed to cease and desist from committing future violations of the relevant provisions of the Securities Act and the Exchange Act, and also agreed to certain undertakings, including cooperation in connection with any further SEC investigation of the matter.

Notably, at this time the SEC has not taken any action against individual executives in connection with Yahoo's disclosure failures; however, the SEC investigation remains ongoing and the language of the Order does not foreclose the possibility of further action being taken.

## Practical Considerations

This enforcement action against Yahoo highlights the SEC's focus on the issue of cybersecurity disclosure practices. While Steven Peikin, Co-Director of the SEC's Enforcement Division, stressed that "[the SEC does] not second-guess good faith exercises of judgment about cyber-incident disclosure" in this case the SEC found the company's response was "so lacking" that an enforcement action was clearly warranted.[6] This first-of-its-kind fine puts companies on notice that the SEC expects companies to inform investors and the marketplace about cyber-incidents on a timely basis and communicates the SEC's intent to hold companies accountable when they delay informing investors about cybersecurity incidents.

Many of the disclosure issues noted in the Order are consistent with the SEC's directives in the New Guidance, and companies should continue to evaluate their practices around cybersecurity and related disclosures in light of that guidance. Specifically, this enforcement action highlights that companies should pay attention to:

---

5 Specifically, Sections 17(a)(2) and 17(a)(3) of the Securities Act and Section 13(a) of the Exchange Act and Rules 12b-20, 13a-1, 13a-11, 13a-13 and 13a-15 thereunder.

6 *See* the SEC's press release, available here.

## Disclosure

- **Risk Factors**: In drafting risk factors, companies should consider where cybersecurity risks and incidents rank in terms of the company's most significant risks, and should include disclosure regarding prior material incidents to the extent such disclosure provides context for the evaluation of cybersecurity risks.
- **MD&A**: Companies should carefully consider whether cybersecurity-related risks could represent an event, trend or uncertainty that is reasonably likely to have a material effect on results of operations, liquidity or financial condition.

## Disclosure Controls and Procedures

Companies should assess whether they have adequate disclosure controls and procedures in place to ensure that cybersecurity risks and incidents are timely identified, evaluated, and reported up the corporate ladder to enable senior management (as well as auditors and outside counsel) to assess and analyze their impact on the company's business and make decisions about whether disclosure is required and whether other actions should be taken.

## Disclosure Timing

The SEC expects companies to report a material cyber incident promptly, and a lengthy ongoing internal or external investigation is not, on its own, an acceptable basis for avoiding disclosure of a material cybersecurity incident.

## Correcting or Updating Disclosure

Companies should be mindful that they may have a duty to correct prior disclosure about a cybersecurity event that the company later determines was not accurate (or omitted a material fact about such an event) at the time it was made, or a duty to update disclosure that becomes materially misleading after it was made and is still being relied on by reasonable investors.

White & Case LLP
1221 Avenue of the Americas
New York, New York 10021-1095
United States

**T** +1 212 819 8200