SQUIRE PATTON BOGGS

Yahoo Fined US$35 Million by SEC for Misleading Investors by Failing to Disclose Cybersecurity Breach in First Case of Its Kind

In a settled order issued on April 24, 2018, the Securities and Exchange Commission (SEC) fined Yahoo US$35 million for failing to properly assess and disclose a 2014 data breach that affected more than 500 million user accounts. The case marks the first time the SEC has charged a public company with cybersecurity-related disclosure violations.

Federal securities laws and regulations impose obligations on public companies to make certain disclosures in reports they file with the SEC, such as risk factors and events, trends and uncertainties reasonably likely to have a materially adverse effect on their business. Public companies must also have sufficient "disclosure controls and procedures" to ensure required information is timely and accurately disclosed.

While there is no specific cybersecurity disclosure requirement in the federal securities laws or the SEC's rules, the SEC has stressed the importance of such disclosure for some time. In 2011, the staff of the SEC's Division of Corporation Finance issued their own guidance to encourage more public companies to communicate their cybersecurity risks to investors in light of the rising threat of cyber incidents and the associated costs for affected companies. In February of this year, the SEC itself issued cybersecurity disclosure guidance, largely building on the staff's 2011 guidance.

At the same time, SEC leaders have hypothesized about potential enforcement actions against public companies that fail to disclose material cyber risks and incidents. In October 2017, Stephanie Avakian, Co-Director of the SEC's Enforcement Division, noted, "We recognize this is a complex area subject to significant judgment, and we are not looking to second-guess reasonable, good faith disclosure decisions, though we can certainly envision a case where enforcement action would be appropriate." Similarly, in a September 2017 speech, SEC Chairman Jay Clayton warned that, "Issuers and other market participants must take their periodic and current disclosure obligations regarding cybersecurity risks seriously, and failure to do so may result in an enforcement action."

Given the facts described in the Yahoo Order, it comes as no surprise that the SEC chose this as the first such action. Despite knowing a monstrous breach had happened, Yahoo included only a fairly vanilla disclosure acknowledging the existence of the possibility of an information security-related risk. Such disclosures are typical and would not indicate any major concerns to an investor. According to the SEC's order, however, Yahoo had already suffered what was then the largest known user data theft in history.

Although the realities of a crisis situation are never as clear as the bullet points cited about it years later, it is worth looking at what Yahoo's Information Security team apparently told executives and legal with no discernible response.

2014

- Russian hackers stole copies of Yahoo's entire user database files
- Database files contained personal information of at least 108 million users and likely Yahoo's entire user database of billions of users
- Personal data included hashed passwords and security questions and answers, along with username, email address, telephone number and date of birth
- 26 Yahoo users' email accounts were targeted because of connections to Russia

2015-16

- Same hackers continuously targeted Yahoo's databases throughout 2015 and 2016
- Entire database likely stolen by nation-state actors via several intrusions, including the 2014 intrusion

According to the SEC, despite having this information, senior management:

- Did not properly assess the scope, business impact or legal implications of the breach
- Did not properly assess whether the breach should have been disclosed in public filings or render any statements in its public filings misleading
- Did not share information with Yahoo's auditors
- Did not share information with Yahoo's outside counsel
- Did not maintain disclosure controls and procedures to ensure information security team reports escalated appropriately for the company to determine risk and disclosure obligations

While the Yahoo case may be an extreme example, it serves as yet another reminder that the SEC remains laser-focused on cybersecurity issues. Public companies should consider reviewing their procedures to identify and evaluate cybersecurity risks and incidents, and should ensure the people involved in drafting and approving public disclosures have sufficient information to make informed and defensible judgments about cyber disclosure. Based on public statements, the SEC seems unlikely to second-guess good faith cyber disclosure judgments, but non-disclosures accompanied by inadequate, or non-existent, disclosure controls seem likely to draw the agency's scrutiny. It is, therefore, critical that information security, executives and legal personnel collaborate, learn from each other, and communicate priorities when it comes to cybersecurity risks and incidents. Knowledgeable outside counsel can help ensure the right questions are asked so that well-informed disclosure judgments can be made.

Contacts

Coates Lear
Principal, Denver
Former Senior Counsel, SEC Division of Enforcement
T +1 303 894 6141
E coates.lear@squirepb.com

Tara Swaminatha
Partner, Washington DC
Former Federal Cybercrime Prosecutor, Department of Justice
T +1 202 457 6031
E tara.swaminatha@squirepb.com