Simpson Thacher

Memorandum

In Its First Settlement With an Issuer for a Disclosure Relating to a Cyber Incident, SEC Imposes $35 Million Fine for Yahoo!'s Failure to Disclose a Cybersecurity Breach

May 1, 2018

On April 24, 2018, the Securities and Exchange Commission announced that Yahoo! Inc. (now known as Altaba) agreed to pay a $35 million penalty to settle charges that it misled investors by failing to disclose a significant data breach in which hackers stole personal data relating to hundreds of millions of user accounts. While the SEC has been making clear that it is focused on the adequacy of cyber-related disclosures, this settlement marks the first time that the SEC has brought a case against an issuer for disclosures relating to a cyber incident. While the SEC did not charge any individual company executives (the SEC's investigation is ongoing), the order does impose a number of non-standard, detailed continuing cooperation obligations on Yahoo!. This settlement follows the Commission's interpretative guidance in February that addressed the provisions of the federal securities laws that may be implicated by cyber incidents and that should be considered when evaluating a cyber incident, cyber-related risk, and related disclosures.

The Yahoo! Breach

The order finds that, in December 2014, hackers breached Yahoo!'s systems and stole usernames, email addresses, phone numbers, birthdates, encrypted passwords, and security questions and answers for hundreds of millions of user accounts. According to the order, Yahoo!'s information security team learned of the intrusion within days of this attack. The order finds that information relating to the breach was reported to members of Yahoo!'s senior management and legal department, but that the company did not disclose the breach to investors until two years later, when Verizon was in the process of acquiring Yahoo!'s operating business.

The SEC's Order

The Commission stated that Yahoo! failed to investigate properly the circumstances of the breach and to consider adequately whether the breach needed to be disclosed to investors. The order includes findings about the company's disclosure violations. First, the company failed to disclose the breach or its potential business impact and legal implications in quarterly and annual reports in the two years following the breach. According to the order, Yahoo!'s public disclosures stated only that it faced the risk of, and negative effects that might flow from, data breaches without also disclosing that an actual breach had occurred. Second, the order cites the 2016 stock purchase agreement between Yahoo! and Verizon that was filed with the Commission as an exhibit to Yahoo!'s current report on Form 8-K. The order finds that Yahoo!'s representations in this stock purchase agreement that the company had not experienced any significant data breaches were materially misleading. Third, the order finds that Yahoo! failed to disclose the breach to its auditors and outside counsel, which according to the order could have enabled those outside entities to assess the company's disclosure obligations. Finally, the order finds that Yahoo! failed to maintain adequate disclosure controls and procedures to evaluate cyber incidents and potential disclosure obligations.

The order concludes that Yahoo! committed the following non-scienter violations: Sections 17(a)(2) and 17(a)(3) of the Securities Act of 1933 and Section 13(a) of the Securities Exchange Act of 1934 and Rules 12b-20, 13a-1, 13a-11, 13a-13, and 13a-15. (The Commission did not find that the Company violated Section 10(b) of the Exchange Act or otherwise acted with scienter.) Yahoo! did not admit or deny the findings, and agreed to pay a fine of $35 million and to cooperate fully with the Commission's ongoing investigation, including producing, without service of a notice or subpoena, non-privileged documents and other materials within 14 days of any Staff request; using its best efforts to make Yahoo!'s current and former directors, officers, and employees agents available for interviews, testimony, and trial; and using its best efforts to ensure that its directors, officers, and employees respond to inquiries relating to any and all investigations and litigations relating to the matter.

The SEC's Ongoing Focus on Cybersecurity

Simpson Thacher's February 22, 2018 memorandum addressed the Commission's recent interpretative guidance concerning public company cybersecurity disclosures. This guidance expanded upon the Division of Corporation Finance's 2011 guidance regarding disclosure obligations related to cybersecurity risks and incidents. The release also addressed two topics not developed in the Staff's 2011 guidance: the importance of cybersecurity policies and procedures and the application of insider trading prohibitions in the cybersecurity context. At the time of our memo, we noted that the Commission had not charged any issuers with respect to disclosure violations relating to cyber incidents but anticipated that, with the issuance of the interpretative guidance, the Commission might be more inclined to pursue cyber-related enforcement actions—on both disclosure and internal controls theories—to validate the principles articulated in the guidance. The Commission's order against Yahoo! reflects its continuing focus on cybersecurity issues. We

expect that after cyber incidents become public, the Commission will investigate actively how issuers discharged their disclosure obligations once the incidents became known.

Given the SEC's focus on cyber security disclosures and related cyber issues, issuers should review their disclosures relating to cybersecurity risks before filing periodic reports and should closely consider whether the periodic report as whole, including any relevant representations or exhibits that could be considered part of the report, adequately discloses material cyber risks and any incidents known to the company. Issuers also should assess whether their current disclosure controls and procedures are comprehensive enough to ensure that relevant information about cybersecurity risks and incidents is reported up the corporate ladder, investigated, and analyzed within sufficient time for the information to be adequately considered (including by the company's disclosure committees and professional advisors) before the issuer makes a periodic filing with the Commission and opens its trading window.

Finally, comments by a co-director of the SEC's Enforcement Division announcing the charges against Yahoo! appear to acknowledge that identifying and assessing cyber risk and disclosure obligations is not always straightforward. The co-director reportedly stated on a conference call with the media that: "It's a difficult judgment call whether, when and how to disclose a breach. . . . We don't seek to second-guess good faith decisions." However, the SEC also reiterated that it will continue to scrutinize cyber-related disclosures. In the press release announcing the Yahoo! settlement, the co-director also stated, "We have also cautioned that a company's response to such an event could be so lacking that an enforcement action would be warranted. This is clearly such a case."

For further information about this development, please contact one of the following members of the Firm:

NEW YORK CITY

Stephen M. Cutler
+1-212-455-2773
stephen.cutler@stblaw.com

Nicholas S. Goldin
+1-212-455-3685
ngoldin@stblaw.com

Karen Hsu Kelley
+1-212-455-2408
kkelley@stblaw.com

Lori E. Lesser
+1-212-455-3393
llesser@stblaw.com

Michael J. Osnato, Jr.
+1-212-455-3252
michael.osnato@stblaw.com

Janice G. Brunner
+1-212-455-3529
janice.brunner@stblaw.com

Jonathan S. Kaplan
+1-212-455-3028
jonathan.kaplan@stblaw.com

WASHINGTON, D.C.

Rajib Chanda
+1-202-636-5543
rajib.chanda@stblaw.com

Simpson Thacher Worldwide

UNITED STATES

New York
425 Lexington Avenue
New York, NY 10017
+1-212-455-2000

Houston
600 Travis Street, Suite 5400
Houston, TX 77002
+1-713-821-5650

Los Angeles
1999 Avenue of the Stars
Los Angeles, CA 90067
+1-310-407-7500

Palo Alto
2475 Hanover Street
Palo Alto, CA 94304
+1-650-251-5000

Washington, D.C.
900 G Street, NW
Washington, D.C. 20001
+1-202-636-5500

EUROPE

London
CityPoint
One Ropemaker Street
London EC2Y 9HU
England
+44-(0)20-7275-6500

ASIA

Beijing
3901 China World Tower
1 Jian Guo Men Wai Avenue
Beijing 100004
China
+86-10-5965-2999

Hong Kong
ICBC Tower
3 Garden Road, Central
Hong Kong
+852-2514-7600

Seoul
25th Floor, West Tower
Mirae Asset Center 1
26 Eulji-ro 5-Gil, Jung-Gu
Seoul 100-210
Korea
+82-2-6030-3800

Tokyo
Ark Hills Sengokuyama Mori Tower
9-10, Roppongi 1-Chome
Minato-Ku, Tokyo 106-0032
Japan
+81-3-5562-6200

SOUTH AMERICA

São Paulo
Av. Presidente Juscelino
Kubitschek, 1455
São Paulo, SP 04543-011
Brazil
+55-11-3546-1000