KATZ, MARSHALL & BANKS, LLP

Yahoo Settlement Reflects Important Role of Cybersecurity Whistleblowers

May 3, 2018

The U.S. Securities and Exchange Commission (SEC) has reached yet another settlement arising from a cybersecurity event. On April 24, 2018, the SEC announced that it had reached a $35 million settlement with Altaba, Inc. – the company formerly known as Yahoo! Inc. – to resolve claims that the company misled investors by failing to disclose the cybersecurity breach that enabled hackers to steal the personal data of hundreds of millions of Yahoo users.

The Yahoo Data Breach

According to the SEC, in December 2014, Yahoo's information security team, including its chief information security officer (CISO), learned of a massive breach of the company's user database resulting in the acquisition of more than 500 million user accounts. The information stolen in the breach included personal data that Yahoo's information security team referred to as the company's "crown jewels": Yahoo usernames, email addresses, telephone numbers, dates of birth, hashed passwords, and security questions and answers.

Within days, the CISO notified members of Yahoo's senior management and legal teams that malicious hackers had acquired hundreds of millions of Yahoo users' personal data. But the individuals on those teams did not share this information with Yahoo's auditors or outside counsel to enable them to assess the company's disclosure obligations in its public filings. As a result, Yahoo's risk factor disclosures in its annual and quarterly reports from 2014 through 2016 claimed the company only faced the risk of *future* data breaches, while failing to disclose that a massive data breach had already taken place.

Yahoo's misleading disclosures continued into 2016 while in talks with Verizon Communications, Inc., about the potential sale of its operating business to Verizon. Yahoo affirmatively represented in a July 23, 2016, stock purchase agreement that it had not experienced any significant data breaches. Yahoo did not disclose the breach until September 2016; the day after its disclosure, the company's market capitalization decreased by nearly $1.3 billion. Yahoo later admitted in a Form 10-K filed on March 1, 2017, that the "relevant legal team had sufficient information to warrant substantial further inquiry in 2014, and they did not sufficiently pursue it."

SEC Public Disclosure Requirements

SEC regulations require the filing of periodic public disclosures and dictate the specific content of those disclosures. Specifically, Item 503(c) of Regulation S-K, codified at 17 C.F.R. § 229.503(c), requires "a discussion of the most significant factors that make the offering speculative or risky." The SEC has explained that Regulation S-K arose from Sections 7, 10, and 19(a) of the Securities Act, and Sections 3(b), 12, 13, 14, 15(d), and 23(a) of the Exchange Act. Guidance documents issued by the SEC in October 2011 and February 2018 make clear that the Commission "expect[s] companies to disclose cybersecurity risks and incidents that are material to investors, including the concomitant financial, legal, or reputational consequences." The February 2018 Guidance continued, "Companies should avoid generic cybersecurity-related disclosure and provide specific information that is useful to

investors.” According to the SEC, Yahoo’s failures to disclose material information violated the Securities Act and the Exchange Act and the related rules and regulations.

Good News for Cybersecurity Whistleblowers

The SEC’s February 2018 Cybersecurity Guidance, along with this settlement, are encouraging news for cybersecurity whistleblowers who are pressuring their companies to either address cybersecurity deficiencies or be more transparent about past or potential data breaches. As Alexis Ronickher explains in more detail in her Cybersecurity Whistleblower Protection Guide, because the securities laws require publicly traded companies to disclose material risks, a cybersecurity whistleblower’s concerns about her company’s failure to disclose such a risk could constitute protected activity under statutes like the Sarbanes-Oxley Act of 2002. Moreover, as this settlement demonstrates, they could also form the basis of a valuable whistleblower tip to the SEC.

This blog was subsequently published in Corporate Compliance Insights.