Bloomberg Law®

Privacy and Security Law Report®

VOL. 17, NO. 0 687-722 JUNE 4, 2018

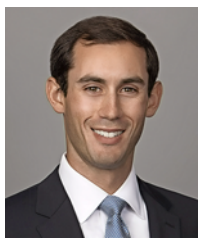
Yahoo Settlement Changes SEC Expectations on Cyber Disclosure

Data Breaches

Public companies should not expect that the SEC will wait for a similarly egregious case to bring future cybersecurity disclosure enforcement actions, attorneys from Cadwalader, Wickersham & Taft LLP write.







By Joseph V. Moreno, Kyle DeYoung, Keith Gerver, Alexander Hokenson, and Stephen Weiss

Joseph Moreno (@JosephMoreno), a former federal prosecutor, is a partner in Cadwalader's White Collar Defense and Investigations Group.

Kyle DeYoung is a partner in Cadwalader's White Collar Defense and Investigations practice, as well as the firm's Corporate and Financial Services Litigation and Regulation Practice.

Keith Gerver (@kgerver) is an associate in Cadwalader's White Collar Defense and Investigations Group.

Alex Hokenson is an associate in Cadwalader's White Collar Defense and Investigations Group.

Stephen Weiss is an associate in Cadwalader's White Collar Defense and Investigations Group.

In its long-awaited, first-ever enforcement action against a public company for failing to disclose a data breach, the Securities and Exchange Commission recently imposed a $35 million civil money penalty against Altaba Inc. (formerly known as Yahoo! Inc.) alleging that the internet media company made materially misleading statements in its public filings by repeatedly neglecting to disclose its 2014 cyber incident to investors.

Yahoo violated Sections 17(a)(2) and 17(a)(3) of the Securities Act of 1933, and Section 13(a) of the Securities and Exchange Act of 1934, according to the SEC's order, by failing to disclose its 2014 data breach in numerous quarterly, annual, and periodic reports over the subsequent two years, and for failing to maintain controls that ensured the breach would be evaluated for potential public disclosure.

The Yahoo data breach involved several factors that made it particularly serious, including a sophisticated cyberattack conducted by Russian hackers and the loss of more than 500 million users' personal information, known according to an SEC press release as Yahoo's ''crown jewels'' (usernames, email addresses, telephone numbers, birth dates, passwords, and security answers). Further, Yahoo's internal security team and senior management knew about the intrusion, but the

 ISSN 1538-3423

company failed to adequately investigate the breach or publicly disclose it for nearly two years. Such a reporting delay portrayed the company in a particularly bad light with regulators.

However, public companies should not expect that the SEC will wait for another similarly egregious case to bring future cybersecurity disclosure enforcement actions and should instead take this opportunity to understand the SEC's expectations for cybersecurity risk and incident disclosures in public filings going forward.

2011 Cyber Disclosure Guidance

The SEC's Division of Corporation Finance issued guidance in October 2011 on reporting obligations for public companies regarding cybersecurity risks and cyber incidents.

The disclosure guidance recognized that the growing reliance of public companies on digital technologies meant that cybersecurity-related risks and events could be sufficiently material to investors such that they may be required to be disclosed in registration statements, financial statements, and other public filings. As a result, it called for public companies to review, on an ongoing basis, the adequacy of their disclosure policies relating to cybersecurity risks and cyber incidents, along with other operational and financial risks.

§ *Cybersecurity Risks*. The disclosure guidance suggested that companies should disclose the risk of cyber incidents if these issues are ''among the most significant factors that make an investment in the company risky.'' In determining whether to report any cybersecurity risks, companies should consider, among other things: (i) the probability of a cybersecurity incident occurring; (ii) the potential magnitude and costs associated with the risk; (iii) prior cybersecurity incidents; and (iv) the adequacy of possible preventative measures. The disclosure guidance cautioned against ''boilerplate'' disclosures and, instead, advised that companies tailor the discussion of their specific cybersecurity risks. It emphasized, however, that companies need not disclose information that would, in itself, compromise its ability to defend against cyberattacks.

§ *Cyber Incidents*. The disclosure guidance also set forth a number of considerations regarding the disclosure of cyber incidents, including whether: (i) the incident will have a material effect on the company's financial condition; (ii) material intellectual property was stolen; (iii) the cyber incident materially affected products, services, or customer relationships; and (iv) the company has been subject to prior data breaches. A company should also consider the impact of remediation costs for stolen assets and information, repairs to internal systems that hackers may have compromised, and the necessity of engaging outside firms to assist with breach response and remediation.

2018 SEC Enhancements

The SEC issued interpretive guidance in February for the stated purpose of not replacing but ''reinforcing and expanding upon'' the disclosure guidance. To that effect, it adds detail to several topics, including:

§ *Materiality Standard*. In determining how general disclosure obligations under federal securities laws apply to cybersecurity, companies should weigh, among other things, the potential materiality of any identified cybersecurity risk and, in the case of cyber incidents, the importance of any compromised information and of the impact of the cyber incident on the company's operations. The materiality of cybersecurity risks or cyber incidents depends on their nature, extent, and potential magnitude, as well as on the range of harm that such incidents could cause to the company's reputation, financial performance, and customer and vendor relationships, and to the possibility of litigation or regulatory actions. In emphasizing that public companies must disclose cybersecurity risks and incidents that are material to investors, the SEC reiterated that companies are not obligated to make disclosures that are so detailed they could compromise the company's cybersecurity efforts. The SEC also emphasized that while an internal investigation may be necessary to ascertain the extent of an incident's materiality, it cannot be used as an excuse to unduly delay disclosures to the investing public.

§ *Risk Factors*. In disclosing significant factors that make investments in the company's securities speculative or risky, companies should disclose the risks associated with cybersecurity and cybersecurity incidents, including those that arise in connection with acquisitions. In evaluating such disclosures, the SEC suggests a number of factors to consider, including the occurrence of prior incidents; the probability of occurrence and potential magnitude of incidents; the adequacy of preventative actions taken; costs; the potential for reputational harm; and the impact of laws, regulations, and litigation.

§ *Management Discussions and Analysis*. The cost of ongoing cybersecurity efforts, the costs and other consequences of cybersecurity incidents, and the risks of potential cybersecurity incidents, among other matters, could inform a company's analysis and discussion of its financial condition, changes in financial condition, and results of operations.

§ *Description of Business*. Companies should disclose if cybersecurity incidents or risks materially affect a company's products, services, relationships with customers or suppliers, or competitive conditions.

§ *Legal Proceedings*. Companies should note that the requirement to disclose information relating to material pending legal proceedings includes any proceedings that relate to cybersecurity issues.

§ *Financial Statement Disclosures*. Companies should ensure that their financial reporting and control systems are designed to provide reasonable assurance that information about the range and magnitude of the financial impacts of a cybersecurity incident would be incorporated into its financial statements on a timely basis as the information becomes available.

  PVLR ISSN 1538-3423

§ *Board Risk Oversight*. To the extent that cybersecurity risks are material to a company's business, any discussion of how the company's board of directors administers its risk oversight function should include the nature of its role in overseeing cybersecurity risk.

In addition, the 2018 interpretive guidance touches on several additional topics of interest:

§ *Disclosure Controls and Procedures*. The 2018 guidance emphasizes the importance of companies maintaining comprehensive policies and procedures related to cybersecurity risks and incidents. Compliance with such policies and procedures should be assessed regularly, including the sufficiency of their disclosure controls and procedures as they relate to cybersecurity disclosure. This includes whether relevant information about cybersecurity risks and incidents is processed and reported up the corporate ladder.

§ *Correcting and Updating Prior Disclosures*. The 2018 guidance also reminded companies that they may have a duty to correct previous disclosures which they later determine to be untrue or misleading. Companies may also have a duty to update previous disclosures that, while accurate at the time of disclosure, have become materially inaccurate since they were made.

§ *Insider Trading*. The new guidance also noted that companies should consider how their codes of ethics and insider trading policies take into account and prevent trading on the basis of material nonpublic information related to cybersecurity risk and incidents. In addition, companies should consider whether and when it may be appropriate to implement restrictions on insider trading while significant cybersecurity incidents are being investigated and assessed. The SEC also noted that companies must ensure compliance with Regulation FD with respect to not selectively disclosing material nonpublic information regarding cybersecurity risks and incidents to insiders before making full disclosure of that same information to the general public.

Conclusion

The SEC's action against Yahoo is its first enforcement action against a company for failing to disclose a cyber breach, and it involved egregious conduct. The details and scope of the Yahoo action may provide insight into how the SEC will evaluate other data breach disclosures, including Equifax's September 2017 data breach disclosure and possibly Facebook's disclosures related to the Cambridge Analytica scandal. Equifax waited approximately five weeks to disclose its breach, where hackers stole Social Security numbers, birth dates, addresses, and driver's license numbers for approximately 143 million individuals, in addition to credit card numbers for more than 200,000 others. The SEC's review of Equifax will likely take into account the weeks-long delay in reporting the cyber incident, as well as the materiality of the breach, how and when Equifax investigated the breach, and company executives allegedly using confidential information to sell stock before publicly disclosing the breach. Similarly, Facebook reportedly waited years before disclosing the incident where Cambridge Analytica inappropriately collected the personal information of up to 87 million users. Although the Facebook incident may not have been a technical data breach, the SEC will likely look closely at the delay in reporting the incident, the materiality of the incident, and how Facebook responded when it learned of the incident.

Public companies may be tempted to look at the egregious nature of the Yahoo breach and believe the bar is high for future disclosure actions, but that may be short-sighted because companies are now on notice as to what the SEC expects in public disclosures. In-house counsel and compliance professionals are strongly advised to familiarize themselves with the SEC cybersecurity risk and incident disclosure expectations, and ensure they have adequate cybersecurity policies, procedures, and internal controls in place to help make sure their public disclosure obligations are met.