McGUIREWOODS

Between a Rock and a Hard Place:

SEC Disclosure Analysis in Light of the Yahoo Settlement

ALEXANDER MARTIN MADRID
412 667 7919 | amadrid@mcguirewoods.com
Tower Two-Sixty
260 Forbes Avenue, Suite 1800
Pittsburgh, PA 15222

DAVID S. WOLPA
704 343 2185 | dwolpa@mcguirewoods.com
201 North Tryon Street, Suite 3000
Charlotte, NC 28202

C. ANDREW KONIA
703 712 5071 | akonia@mcguirewoods.com
1750 Tysons Boulevard, Suite 1800
Tysons, VA 22102

JANE WHITT SELLERS
804 775 1054 | jsellers@mcguirewoods.com
800 East Canal Street
Richmond, VA 23219

May 8, 2018
www.mcguirewoods.com

Summary

On April 25, the Securities and Exchange Commission announced a settlement with Yahoo that constituted its first enforcement action against a public company for failing to disclose a data breach. The settlement demonstrates that companies in post-data breach environments must engage in a thorough, fulsome analysis of whether to disclose the cybersecurity incident in their public filings.

In conducting this analysis, companies face a difficult choice: disclose and face public and investor backlash, or decline to disclose and potentially face later regulatory scrutiny and/or class action stockholders' litigation.

This article analyzes what the Yahoo settlement can teach about proper disclosure analysis and discusses factors a company must consider when conducting this critical task.

The April 25 announcement by the SEC of its cease-and-desist Order and accompanying $35 million fine against Yahoo! Inc. (now Altaba Inc.) has generated significant attention from industry commenters. The investigation, conducted by the SEC's new Cyber Unit, led to the agency's first enforcement action against a public company for failing to disclose a data breach. As has been widely reported, the SEC's Order made factual findings — which Yahoo neither admitted nor denied — that Yahoo's information security team, including its Chief Information Security Officer, knew by December 2014 that hackers associated with the Russian Federation had breached Yahoo's security and stolen copies of user database files containing the personal data of at least 108 million users. According to the Order, the theft was reported to Yahoo's senior management and legal teams, but Yahoo failed to disclose the breach, instead representing in repeated public filings throughout 2015 and 2016 that it was unaware of any security breaches that would have a material adverse effect on its business. After Yahoo's ultimate disclosure of the breach in September 2016, its share price tumbled and its market capitalization decreased by almost $1.3 billion. The disclosure was also followed by a $350 million reduction in the acquisition price that Verizon paid for Yahoo's operating business.

Lessons Learned

As the dust settles on initial reactions to the settlement announcement, attention must turn to the lessons that can be learned from what happened at Yahoo and the SEC's enforcement action. The Yahoo settlement demonstrates the importance, and difficulty, of engaging in a thorough, fulsome disclosure analysis. Although federal law does not require a company to publicly announce a data breach in every case, public companies are obligated not to make materially misleading statements and to disclose such further material information as may be necessary to make the statements made, in light of the circumstances under which they were made, not misleading.

Accordingly, upon discovery of a breach, a public company must make a careful evaluation of whether to disclose the breach, or whether hurried disclosure of an event that turns out to be objectively immaterial could have otherwise avoidable material adverse consequences. On the one hand, should the company choose not to disclose, it risks potential class action litigation or a future enforcement action if a regulator later determines the breach should have been disclosed; on the other hand, if the company chooses to disclose, it may face public and investor backlash (and potential class action litigation), even if such responses are unwarranted. For many companies, navigating between these two outcomes proves as difficult as steering between the Scylla and Charybdis of Greek mythology — avoiding one disastrous outcome may lead to another that is equally painful.

Nevertheless, the importance of engaging in a careful disclosure analysis cannot be overstated. The analysis not only allows senior management and the company's counsel to properly scope the breach and develop an appropriate remediation plan, but also serves as a defense in the event of subsequent regulatory inquiries. Indeed, closely read, the Order

demonstrates the SEC's view that Yahoo's failure to conduct a proper disclosure analysis was at least as problematic as its failure to timely disclose.

KEY TAKEAWAY

The failure to conduct a proper disclosure analysis can be at least as problematic to the SEC as the failure to timely disclose.

The Order finds that even after Yahoo's senior management was made aware of the theft of user data, it "did not properly assess the scope, business impact, and 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." The Order further faults Yahoo management for failing to share information regarding the breach with "Yahoo's auditors or outside counsel in order to assess the company's disclosure obligations in its public filings." Steven Peikin, Co-Director of the SEC Enforcement Division, explained upon the announcement of the settlement that while the SEC will not "second-guess good faith exercises of judgment about cyber-incident disclosure," where a company's response to a breach is found "lacking" an enforcement action "would be warranted." This comment emphasizes the SEC's position that Yahoo's failure to perform a fulsome disclosure analysis constituted a response that was "lacking" in judgment and warranted an enforcement action.

Proper Manner and Method

Yet even as the SEC emphasizes the importance of disclosure analysis, the proper manner and method by which this analysis must be undertaken remains an evolving target. In February, the SEC provided guidance on public companies' disclosure obligations regarding cybersecurity risk and incidents. This guidance was principally framed in terms of how disclosure may be required under the SEC's existing rules requiring discussions of risk factors, management's discussion and analysis of financial conditions and operations, and the traditional materiality analysis. In this regard, it was somewhat similar to guidance issued by the SEC's Division of Corporation Finance in 2011, but qualitatively different in that the 2018 guidance came at the Commission level. Two members of the Commission criticized the guidance as failing to meaningfully build upon the previously issued guidance; their preference was for the Commission to adopt explicit rules regarding cybersecurity, rather than relying on the existing disclosure framework to ensure proper disclosure is made. In particular, Commissioner Kara Stein called for the occurrence of a cybersecurity incident to be a mandatory disclosure event under Form 8-K (which must be filed within four business days of the occurrence of the event), which would remove a significant amount of discretion from a company's management regarding its disclosure decision — although materiality likely would still be the predominant consideration were such a requirement ever put in place. It should be noted that many companies already include disclosures regarding the risks posed by cybersecurity attacks in their risk factors and forward-looking statement disclaimers in

their annual reports on Forms 10-K and other periodic reports, but when and how a company should disclose the actual occurrence of a breach and its possible repercussions can be a difficult evaluation.

The factors a company should consider when determining whether and how to disclose a data breach vary depending upon circumstances, and companies are encouraged to consider retaining outside counsel to assist in the analysis. However, the Yahoo settlement informs and reiterates important elements of the analysis that are broadly applicable in post-breach determinations of whether to disclose. First, following a data breach, companies should conduct a materiality analysis. The SEC's finding that Yahoo's data breach was material to investors and therefore should have been disclosed on that basis should cause companies to reconsider the utility of this analysis. The materiality analysis should consider multiple issues, both individually and in the aggregate:

Costs | Companies should consider the likely cost of the breach as part of a documented financial analysis. The SEC's February guidance provided a non-exhaustive list of costs that companies may incur from a breach, such as remediation costs, costs to harden systems and increase protection, lost revenue, litigation or regulatory investigation costs, and increased premiums for maintaining cybersecurity insurance coverage. Certain costs must be borne regardless of whether the breach is disclosed (such as remediation costs), whereas others are incurred only upon disclosure (such as litigation costs). Companies should consider which of these costs they will actually bear depending on whether they actually disclose. This factor also depends on the size of the company, given that remediation costs will have a much greater impact on the bottom line of smaller companies.

Vulnerability to Future Events | In many cases, upon the initial discovery of a breach, it may be difficult to determine exactly how the breach occurred. However, companies should attempt to determine if the vulnerability that led to the breach has been contained or if they risk further intrusion, whether related to the incident in question or otherwise. This analysis, in turn, informs broader evaluations of the likely impact and cost of the breach. Additionally, companies may need to disclose past breaches, possibly those that were not material, to place the discussion of the company's cybersecurity risk profile in context.

Value of the Information Compromised | Companies should also consider the underlying value of the information compromised. Although the cost to remediate a breach of

POST-BREACH DISCLOSURE FACTORS

A company in a post-breach environment must engage in a careful disclosure analysis requiring consideration of:

Materiality
- Costs
- Vulnerability to future events
- Value of the information compromised
- Likely consequences
- Relevant comparisons

Whom to Brief
- Board
- Counsel
- Auditors

Timing
- Form 8-K
- Quarterly Report

personally identifiable information may be the same as for a breach of purely technical information, the former is far likelier to lead to significant consequences. By the same token, if a company operates critical infrastructure — such as air traffic control or an electric grid — the important nature of the systems breached should be considered.

Likely Consequences | Hand in hand with a company's analysis of the value of the information compromised is a consideration of the likely consequences of the breach. Among the potential consequences that companies must consider are compromised intellectual property, loss of competitive advantage and impact on customer-vendor relationships. The consideration also involves, among other factors, an evaluation of the number of individuals potentially affected by the breach. The company should also weigh the potential for reputational consequences that may result from disclosure of the breach.

Relevant Comparisons | The company should consider whether other comparable companies have experienced similar incidents and what actions those companies took in those cases.

Aside from the materiality analysis, companies face other questions in a post-breach environment as part of the overall decision of whether to disclose the breach. As the SEC's guidance indicated, the company must consider ***who should be informed*** of the breach, including whether the board or the board committee responsible for risk oversight must be briefed. Notably, the SEC in its Order faulted Yahoo for failing to disclose the breach to its auditors and outside counsel. This is because auditors and outside counsel are considered "gatekeepers" in the disclosure landscape. If they are not made aware of the event, they cannot assist the company with these determinations. Companies must make early determinations of whom to involve upon the discovery of the breach so as to ensure that all potential factors of the disclosure analysis are properly considered. Failing to properly advise senior management, the board and/or key outside advisers, such as securities counsel and a company's independent registered public accountants, may demonstrate ineffective disclosure controls and procedures.

Once a company determines that a data breach or other cybersecurity incident is material to investors, the company must then decide ***when to disclose*** the matter. Companies are required to publicly disclose the occurrence of certain specified events within four business days of their occurrence on a Current Report on Form 8-K. Absent an affirmative duty to speak in a Form 8-K or other required report, public companies have no general duty to continuously disclose material information. However, the New York Stock Exchange and the NASDAQ Stock Market each have rules requiring that listed companies release to the public any news that might reasonably be expected to materially affect the market for that company's securities, although these rules are not read as imposing a continuous disclosure regime.

Accordingly, the most logical place to disclose the occurrence of a cybersecurity incident may be in the company's next quarterly (or annual, if in the fourth quarter) report. Most

companies are required to update their risk factors on a quarterly basis, and all companies must disclose known trends or uncertainties with regard to net revenues or liquidity, which might be impacted by a data breach, in "Management's Discussion and Analysis of Financial Condition and Results of Operations" (MD&A). In fact, it was Yahoo's failure to disclose the 2014 breach in its risk factors and MD&A, which are updated only quarterly, that merited the most attention from the SEC.

Nevertheless, there may be reasons why a company would be better off disclosing an event at an earlier time. For example, if the event was becoming widely known, both inside the company and outside, the company should make public disclosure to prevent information imbalances from affecting the market for its securities. Additionally, if the incident is material, knowledge of it constitutes material nonpublic information, the possession of which prohibits trading by company insiders and those with a duty to the company under the insider trading rules. Disclosing early lessens the risk of prohibited insider trading. A company involved in a securities offering in which the company's prior statement of its risk factors and/or MD&A — which do not discuss the new incident — is being incorporated into a prospectus would also be obligated to disclose, since failing to do so could be a material omission. In short, serious consideration of the company's particular situation is needed to properly determine the best time to disclose.

Companies face difficult questions in a post-breach environment. Among these questions is whether and how to disclose the breach to investors and the public. The SEC's settlement with Yahoo teaches important lessons regarding proper disclosure analysis that companies should carefully consider if and when they face a cybersecurity event.

McGuireWoods LLP

McGuireWoods' Securities Compliance and Data Privacy and Security teams work hand-in-hand to advise clients on proper disclosure analyses when a data breach occurs.

Our more than 50 securities compliance lawyers provide experienced guidance and counsel to companies of all sizes, from Fortune 500 organizations to smaller reporting companies. We assist companies listed on various exchanges, including NASDAQ, the NYSE, AMEX and AIM. We work with clients in a range of industries, notably consumer products, energy, financial services, hospitality, manufacturing, retail, technology and transportation, and understand the industry-specific issues that affect our clients and their required reporting.

Recently named a "Leading Cybersecurity Law Firm" by top legal decision-makers at companies with $1B+ in revenue by BTI Consulting (2017), the firm's Data Privacy and Security team provides proactive counseling and investigative and remediation services that may be required after a security breach. Visit our blog *Password Protected* to stay up to date on data privacy and security news and trends.