Cooley

Can Hypothetical Risk Factors Be Misleading?

July 6, 2021

In In re Alphabet Securities Litigation, the State of Rhode Island, as lead plaintiff, filed a Rule10b-5 action against Google LLC, its holding company Alphabet, Inc., and certain executives, alleging that the defendants failed to timely disclose certain cybersecurity defects and vulnerabilities. The district court granted defendants' motion to dismiss the complaint, but on appeal, a three-judge panel of the 9th Circuit reversed in part, holding that the complaint "plausibly alleged" that the decision to omit information about these cybersecurity vulnerabilities "significantly altered the total mix of information available for decision-making by a reasonable investor" and that scienter—intent to deceive, manipulate or defraud—was adequately alleged. Importantly, the Court held that the complaint contained a plausible allegation that Alphabet's omission was materially misleading: its risk factor discussion of cybersecurity was framed in the hypothetical, while, it was alleged, the "hypothetical" events had in fact already come to fruition. The case serves as a reminder of a couple of now-familiar themes: companies need to regularly review their risk factor disclosures, even when—or perhaps especially when—they are incorporating them by reference to ensure that they have been appropriately updated to reflect actual events that may have made the risks described as merely hypothetical no longer so. It's also notable that this case represents the second recent instance of allegations of failure to disclose the discovery of a material cybersecurity "vulnerability"—in the absence of a cyberattack—with disclosure ultimately compelled by the publication of an article exposing the defects. It's another reminder that companies need to be vigilant for potential disclosure obligations about cybersecurity that might arise outside the context of cyberattacks and hacks—in the more-difficult-to-assess context of cybersecurity *vulnerabilities*.

Background

According to the opinion, which, at this stage, assumes the facts plausibly alleged in the complaint, in March 2018, Google discovered that there was a vulnerability in its Google+ social network that had, for three years, left private data of hundreds of thousands of users exposed to third-party developers. As described by the Court, Alphabet and Google, after being warned by their "legal and policy staff that disclosure of these issues would result in immediate regulatory and governmental scrutiny,…chose to conceal this discovery, made generic statements about how cybersecurity risks could affect their business, and stated that there had been no material changes to Alphabet's risk factors since 2017." The question before the Court was whether the complaint adequately alleged that, by omitting to disclose these security problems, the defendants made materially misleading statements in a Form 10-Q and did so with scienter.

According to the Court, since its IPO in 2004, Google has touted the importance of security—user privacy and user trust—to its business. The Court noted that Alphabet's CFO remarked in February 2018 that "security is 'clearly what we've built Google on,'" and its Form 10-K warned of the damage that could result in the event of a cybersecurity breach or privacy violation. In the Spring of 2018, a public scandal involving the improper harvesting by a research firm of user data from an unrelated company led to increased scrutiny of data security practices of large social media companies, including Congressional oversight hearings. The Court also noted that Google had reaffirmed its commitment to comply with the GDPR (the European framework for regulating data privacy protections), which required prompt disclosure of personal data breaches not later than 72 hours after learning of the breach.

Around the same time, the Court said, internal Google investigators discovered a "software glitch in the Google+ social network that had existed since 2015 (referred to in the complaint as the 'Three-Year Bug')," that allowed third-party developers to access and collect some "users' profile data even if those users had relied on Google's privacy settings to designate such data as nonpublic. The exposed private profile data included email addresses, birth dates, gender, profile photos, places lived, occupations, and relationship status." Moreover, it was alleged, a record-keeping limitation prevented Google from reviewing more than the two most recent weeks of user data access, with the result that Google could not determine how many third parties had accessed the data. The investigation into the Three-Year Bug was alleged to have also turned up other vulnerabilities.

As alleged in the complaint, in light of the discovery of these vulnerabilities, Google's legal and policy staff prepared the "Privacy Bug Memo," a memo warning that disclosure of these security issues "would likely trigger 'immediate regulatory interest'" and put the spotlight on the defendants. As a result, the complaint alleged, key officers and directors, including some of the defendants, "chose a strategy of nondisclosure," and Google's CEO "approved a plan to conceal the existence of the Three-Year Bug and other security vulnerabilities." In addition, the Google and Alphabet CEOs

"approved a plan to shut down the Google+ consumer platform," a platform with 395 million monthly active users.

Nevertheless, according to the Court, Alphabet's Form 10-Q for the period ended March 31, 2018, incorporated the risk factor disclosures from its 2017 Form 10-K and did not update to disclose the Three-Year Bug or other security vulnerabilities that had been discovered, specifically stating that there were "no material changes to our risk factors since our Annual Report on Form 10-K for the year ended December 31, 2017." Likewise, it was alleged, no disclosures of the vulnerabilities were made on the earnings call or in the subsequent 10-Q. The same omission continued, it was alleged, in various statements by Google, Alphabet and their employees regarding security and privacy until October 2018.

On October 8, 2018, the *WSJ* published a story exposing "Google's discovery of Google+'s security vulnerabilities and its decision to conceal those vulnerabilities." According to the Court, when "the news broke, Google published a blog post acknowledging the 'significant challenges' regarding data security identified in the Wall Street Journal article." Senators of both parties wrote letters demanding investigations or criticizing the company for withholding information. As recited by the Court from the complaint, "Alphabet's share price fell $11.91 on October 8, $10.75 on October 9, and $53.01 on October 10."

Sidebar

Earlier this month, the SEC brought charges against First American Financial Corporation for failure to timely disclose a cybersecurity *vulnerability*. According to the SEC's order, in May 2019, the company was advised by a journalist that its application for sharing document images related to title and escrow transactions had a vulnerability that exposed "over 800 million title and escrow document images dating back to 2003, including images containing sensitive personal data such as social security numbers and financial information." That evening, the company issued a public statement and, on the next trading day, furnished a Form 8-K to the SEC. However, as it turns out, the company's information security personnel had already identified the vulnerability in a report of a manual test of the application about five months earlier, but failed to remediate it in accordance with the company's policies. They also failed to apprise senior executives about the report, including those responsible for making public statements, even though the information would have been "relevant to their assessment of the company's disclosure response to the vulnerability and the magnitude of the resulting risk." The company was found to have violated the requirement to maintain disclosure controls and procedures and ordered to pay a penalty of almost a half million dollars. As in *Alphabet,* there was no suggestion of a cyberattack or hack; rather, the case involved simply the detection of flaws in the company's application that left the data exposed. (See this PubCo post.)

Three days after publication of the article, securities fraud litigation was filed. The district court granted Alphabet's motion to dismiss for failure to state a claim "after determining that the complaint failed to allege any material misrepresentation or omission and failed to allege scienter sufficiently. Further, the court held that because the Section 10(b) claim failed, the Section 20(a) claim for controlling-person liability 'necessarily fails.'" Rhode Island, as the lead plaintiff, appealed.

A three-judge panel of the 9th Circuit reviewed the case *de novo.* Under decisions of SCOTUS, the Court said, a typical 10b-5 case based on material misrepresentations or omissions requires the plaintiff to prove "(1) a material misrepresentation or omission by the defendant; (2) scienter; (3) a connection between the misrepresentation or omission and the purchase or sale of a security; (4) reliance upon the misrepresentation or omission; (5) economic loss; and (6) loss causation." Only the first two elements were at issue in the case. To satisfy the first element, the Court maintained, "the plaintiff must prove both that the omission is misleading and that it is material." Applying the "objective standard of a 'reasonable investor,'" the Court evaluated whether the omission relating to cybersecurity was materially misleading, taking into account the SEC's interpretive guidance regarding the adequacy of cybersecurity-related disclosures. (See this PubCo post and this Cooley alert.) Scienter can be established by satisfying the standard of "deliberate recklessness," defined as "'an extreme departure from the standards of ordinary care,' which 'presents a danger of misleading buyers or sellers that is either known to the defendant or is so obvious that the actor must have been aware of it.'" The plaintiff must also satisfy the pleading standards of the PSLRA.

The Court focused on two statements made by Alphabet in its Forms 10-Q filed in April 2018 and July 2018:

> "The April 2018 report for the period ending March 31, 2018, stated that Alphabet's 'operations and financial results are subject to various risks and uncertainties,' including those identified in Alphabet's Annual Report on Form 10-K for the year ended December 31, 2017, and asserted that 'here have been no material changes to our risk factors since our Annual Report on Form 10-K for the year ended December 31, 2017.' The 2017 10-K had warned, among other things, that even unfounded concerns about Alphabet's 'practices with regard to the collection, use, disclosure, or security of personal information or other privacy related matters' could damage the company's 'reputation and adversely affect operating results.' Alphabet's April and July 2018 10-Qs make no

mention of the Three-Year Bug or other security vulnerabilities identified in the Privacy Bug Memo."

Because the April 10-Q was filed after the detection of the cybersecurity issues and following the executive deliberations based on the Privacy Bug Memo, as well as the public scandal involving a different company, the Court concluded that the complaint "plausibly alleges that the omission of any mention of the Three-Year Bug or the other security vulnerabilities made the statements in each Form 10-Q materially misleading to a reasonable investor and significantly altered the total mix of information available to investors." The Court also concluded that the complaint plausibly alleged that Alphabet's omission was material, given the various warnings about the potential consequences that could flow from cybersecurity vulnerabilities, as well as the SEC guidance on cybersecurity disclosure.

Importantly, the Court found that the complaint contained a plausible allegation that Alphabet's omission was misleading because the discussion of risks was in the hypothetical, while, it was alleged, the events had actually occurred: "Risk disclosures that 'speak the reader that some of these risks may already have come to fruition' can mislead reasonable investors." As in a number of cases cited by the Court in support, the Court concluded that the "complaint plausibly alleges that Alphabet's warning in each Form 10-Q of risks that 'could' or 'may' occur is misleading to a reasonable investor when Alphabet knew that those risks had materialized."

To Alphabet's contention that the omission from the Forms 10-Q was not misleading because Google had already remediated the software glitch by the time it made the statements, the Court reasoned that, for a business model that requires consumer trust, remediation did not eliminate the "material implications of a bug that improperly exposed user data for three years," including "erosion of consumer confidence and increased regulatory scrutiny." The duration of the glitch and Google's inability to accurately determine the scope, "indicated that there were significant problems with Google's security controls." Alphabet also contended that the 10-Q omissions were not material because there was no release of sensitive financial or medical information or harm to any user and in view of Alphabet's significant revenue increase between 2017 and 2018. But, the Court concluded, that was not determinative: "a cybersecurity incident may be material even if it does not compromise sensitive financial or medical information or have an immediate financial impact on the company. The standard is whether there is a 'substantial likelihood' that the information at issue 'would have been viewed by the reasonable investor as having significantly altered the total mix of information made available for the purpose of decision-making by stockholders concerning their investments.'….Because cybersecurity incidents may cause a range of substantial costs and harms, reasonable investors would likely find omissions regarding significant cybersecurity incidents material to their decision-making." In this case, the complaint alleged that, following publication of the *WSJ* article, there was "a swift stock price decline, legislative scrutiny, and public reaction," all of which, the Court concluded, supported the allegation of materiality.

Sidebar

The SEC has also discussed the dangers of "hypothetical" risk disclosure in another context. CF Disclosure Guidance Topic No. 8, which relates to Intellectual Property and Technology Risks Associated with International Business Operations, provided guidance regarding disclosures that Corp Fin believes companies should consider with respect to intellectual property and technology risks that could arise in connection with international operations, especially in locations where protection of intellectual property may be a bit dicey. The guidance encourages each company to assess these risks and consider their potential impact on its business, financial condition and results of operations, and reputation, stock price and long-term value. Notably, the guidance expressly states that "*where a company's technology, data or intellectual property is being or previously was materially compromised, stolen or otherwise illicitly accessed, hypothetical disclosure of potential risks is not sufficient to satisfy a company's reporting obligations."* (See this PubCo post.)

And the SEC has also brought actions on the same basis. In a complaint filed by the SEC against pharma Mylan N.V., among other things, the SEC alleged that Mylan's risk factor disclosure was misleading: it had framed a claim by the government that Mylan had misclassified its biggest product, the EpiPen, as a "generic," overcharging Medicaid by hundreds of millions of dollars, as a hypothetical possibility, when, in fact, the claim had already been made. More specifically, Mylan did not disclose the claim or the investigation in its risk factors, instead stating only that the government "may take a position contrary to a position we have taken," and that the government may find its submissions to be incorrect. However, the government had already taken a contrary position and asserted that the submissions were wrong. Framed as hypotheticals, the SEC charged, these risk factors were misleading. As a consequence of these and other failures, the SEC alleged, Mylan's SEC filings were false and misleading in violation of the Securities Act and Exchange Act. Mylan agreed to pay $30 million to settle the SEC's charges. (See this PubCo post

.)

To show scienter, the Court observed, the complaint must plausibly allege that "the maker of the statements knew about the security vulnerabilities and intentionally or recklessly did not disclose them." In addition, in this context, the Court said, "scienter of the senior controlling officers of a corporation may be attributed to the corporation itself." Because the complaint alleged that senior executives, including defendant executives, knew about the Three-Year Bug and other vulnerabilities and were aware of and had considered the Privacy Bug Memo, the "complaint's allegations, read as a whole, raise a strong inference that Alphabet was aware" of this information and the consequences of disclosure before filing the 10-Qs. For the same reasons, the Court concluded, "there is an equally strong inference that, armed with this knowledge, Alphabet intentionally did not disclose the cybersecurity information to the public in order to avoid or delay the impacts disclosure could have on regulatory scrutiny, public criticism, and loss of consumer confidence….he competing inference that Alphabet knew of this information but was merely negligent in not disclosing it is not plausible." Nor did the Court buy the argument that the absence of allegations about suspicious insider stock sales implied that Alphabet did not intentionally omit the disclosure from its 10-Q.

In light of these conclusions, the Court reversed the district court's dismissal of the claims related to statements in Alphabet's 10-Q (as well as the dismissal of the complaint's control person claims), holding that the plaintiff adequately alleged falsity, materiality and scienter with respect to the statements in the April 2018 and July 2018 10-Qs. The Court affirmed the lower court's dismissal with regard to a number of other statements, because, as opposed to the statements in the 2018 10-Qs, these statements "did not include the express assurance that there had been 'no material changes' to Alphabet's risk factors since the 2017 10-K filing," or amounted to just "vague and generalized corporate commitments, aspirations, or puffery that cannot support statement liability under Section 10(b) and Rule 10b-5(b)." Hat tip to thecorporatecounsel.net blog.

Contributors