DORSEY
DORSEY+WHITNEY LLP

Cybersecurity, False Statements and Omissions

Cybersecurity and the related disclosures can be critical issues for any company in today's environment. This question is at the center of a recent decision by the Fourth Circuit Court of Appeals. Specifically, the Court focused on the question of what constitutes a false statement in an action centered on cybersecurity claims where information was allegedly omitted. *In re Marriott International, Inc.,* No. 21-1802 (4th Cir. Decided April 21, 2022).

Related Capabilities

- Privacy & Social Media
- Securities & Financial Services Litigation & Enforcement

Factual background

In 2016 Marriott merged with Starwood Hotels. Marriott subsumed all of the operations. Two years later Marriott learned that malware had impacted about 500 million guest records in the Starwood reservation database. That resulted from the second largest data breach in history. This case was filed alleging 73 separate public statements that were false and misleading within the meaning of Exchange Act Section 10(b) and Rule 10b-5 thereunder.

The district court granted Marriott's motion to dismiss with prejudice. The court concluded that Plaintiffs had failed to adequately allege a false or misleading statement or omission. On appeal the Fourth Circuit affirmed.

The decision

On appeal Plaintiffs narrowed their the claims to three groups of statements: 1) those regarding the importance of protecting customer data; 2) a group of privacy statements on Marriott's website; and 3) cybersecurity-related disclosures. To demonstrate that one of the statements in these groups is false and misleading within the meaning of Section 10(b) and the Rule, plaintiff must identify a "factual statement or omission – that is, one that is demonstrable as being true or false." (citations omitted). Stated differently, the challenged statement or omission must be about something consequential . . . material."

Not all material omissions are actionable, the Court noted. Section 10(b) does not

impose a duty to disclose. Rather, the statement is only actionable if a reasonable investor reading it would be misled – that is, the statement is essentially a half-truth. Here none of the identified statements are actionable.

The first group of statements involve the importance of data protection to Marriott's business. Marriott repeatedly states, for example, that "'the integrity and protection of customer, employee, and company data is critical to us . . ." These statements create the impression, according to Plaintiffs, that Marriott was securing and protecting customer data acquired from Starwood . . ." This, however, is not a false statements, according to the Court. Indeed, the basic truth of the Marriott statement – essentially a general fact – is not false or misleading. This is evident from the fact that Marriott made no characterization in the statements.

The second group of statements focus on privacy. Marriott posted statements noting that it seeks to "use reasonable organizational, technical and administrative measures to protect" personal data" but no system is 100% fool proof. Here again, there is nothing that demonstrates these statements are not true.

Statements in the last group are simply broad pronouncements that "no reasonable investor could have been misled by," according to the Court. Included in this group were statements such as those noting that Marriott keeps personal data in a form that permits its use by the firm but it is only maintained for a long as necessary. Again, there is nothing false and misleading about these statements.

In the end, this claim, like the contention that Marriott's cybersecurity risk disclosures are materially misleading because they disclose only risks that have occurred misses the mark. While listing factors that speak of risks that might occur when in fact they have happened may well be misleading, that is not the case here. The disclosures by Marriott speak of risks in the future while acknowledging those that have occurred in the past. Those admissions ensure that the risk factors are not misleading. While Marriott could have added additional detail the "SEC advises companies against 'mak[ing] detailed disclosures that could compromise [their] cybersecurity efforts . ." For these reasons the decision of the district our was affirmed.

Comment

It is axiomatic that Exchange Act Section 10(b) and Rule 10b-5 do not create a duty to disclose. Thus in omission cases the focal question becomes if the additional material must be disclosed. If the omitted information is material and a necessary addition to the statements made so that investors are not misled, then as the Court states here the information must be disclosed. That was not the case here. Indeed, much of the information Plaintiffs claimed should have been viewed as material omissions might have been seenas general background information or risk factors which flagged certain items for investors.

What was not discussed by the Court is situations where there was an affirmative obligation to disclose the information. Decisions such as the Supreme Court's decision in

Affiliate Ute Citizens v. U.S., 408 U.S. 128 (1972) and are keyed to the question of when there is a duty to disclose which is often a function of the relationship between the parties.