Securities Litigation Alert

Akin Gump
STRAUSS HAUER & FELD LLP

Fourth Circuit Rules Omission of Marriott's Data Vulnerabilities Not Actionable Because Challenged Statements Were Not False When Made

May 3, 2022

Key Points

- Fourth Circuit points to SEC guidance on "less is more" approach to cybersecurity disclosures, while finding such disclosures did not violate federal securities laws.
- Omissions of data vulnerabilities were not actionable because the challenged statements were not false when made.
- Although investors argued statements about the "importance" of data security to Marriott were false and misleading, the statements were not actionable because the Court held that Marriott did not "assign a quality to Marriott's cybersecurity that it did not have."
- Marriott's "sweeping caveats" regarding cybersecurity risks ensured no investor could be misled regarding the risks outlined.
- Forward-looking generalized risk disclosures that cybersecurity issues "may" occur were not actionable even though some of those risks had been realized, because Marriott also disclosed it had experienced such challenges.

Summary

Although Marriott could have provided additional information to investors regarding its cybersecurity risks following a merger with Starwood, the federal securities laws did not require it to do so, and Securities and Exchange Commission (SEC) guidance advises companies against detailed disclosures that could compromise their cybersecurity efforts.

Even though Marriott had already experienced some cybersecurity incidents at the time some of the challenged statements were published, its general forward-looking disclosures of cybersecurity risks and "sweeping caveats" shielded it from liability because it also disclosed the challenges it faced and the statements were not false when made.

Contact Information

If you have any questions concerning this alert, please contact:

Natasha G. Kohne
Partner
nkohne@akingump.com
San Francisco
+1 415.765.9505

M. Scott Barnard
Partner
sbarnard@akingump.com
Dallas
+1 214.969.4299

Michelle A. Reed
Partner
mreed@akingump.com
Dallas
+1 214.969.2713

Matthew Vernon Lloyd
Counsel
mvlloyd@akingump.com
Dallas
+1 214.969.4776

Jessica Jones Mannon
Associate
jmannon@akingump.com
Dallas
+1 214.969.2876

Background

In 2016, Marriott merged with Starwood Hotels and Resorts Worldwide. This merger included incorporating all Starwood computer systems and sensitive personal information stored in Starwood databases. Two years later, Marriott learned malware impacted 500 million guest records in Starwood's guest reservation database, constituting the second largest data breach in history at the time.

A putative class action was filed against Marriott and nine of its officers and directors, alleging Marriott's failure to disclose the serious vulnerabilities in 73 different public statements made the statements false or misleading in violation of Section 10(b) of the Securities Exchange Act of 1934 and SEC Rule 10b-5. The investors also brought a claim for secondary liability against the executives under Section 20(a) of the 1934 Act.

The district court granted Marriott's motion to dismiss with prejudice. The district court found that the complaint failed to adequately allege a false or misleading statement or omission, loss causation or scienter.

The investors appealed the ruling with respect to 18 of the original 73 challenged statements.

Opinion

The 4th Circuit affirmed dismissal of the Complaint, finding that none of the alleged misstatements or omissions were false when made or material. The 4th Circuit's analysis began with a critical point: Not all material omissions are actionable. Instead, they must be both material and misleading. Apr. 21, 2022 Order at 4, *Const. Lab. Pen. Tr. For S. Cal. v. Marriott Int., Inc*., No. 21-1802 (4th Cir. Apr. 21, 2022).

On appeal, the investors focused on three categories of statements:

- Statements about the importance of protecting customer data.
- Privacy statements on Marriott's website.
- Cybersecurity-related risk disclosures.

Regarding the importance of customer data, investors argued that Marriott's failure to disclose the vulnerable state of Starwood's IT systems, while repeatedly stating that "the integrity and protection of customer, employer, and company data is critical to us" in Marriott SEC filings, created "the misleading impression that Marriott was securing and protecting customer data acquired from Starwood." *Id*. at 6. But, the Court noted, there is a "basic problem" with the complaint—the facts it alleged did not contradict Marriott's public disclosures. *Id*. Unlike cases where statements touting the strength of systems that are actually false, such as in *In re Equifax Inc. Sec. Litig*., 357 F. Supp. 3d 1189, 1220 (N.D. Ga. 2019), Marriott "did not assign a quality to Marriott's cybersecurity that it did not have." Order at 6. Instead, its public filings merely acknowledged that Marriott considered cybersecurity to be important.

Similarly, the investors' arguments about a series of privacy statements on Marriott's efforts to keep personal data safe failed because they were accompanied by "such sweeping caveats that no reasonable investor could have been misled by them." *Id*. at 8.

The Court held that the third category of arguments—that cybersecurity risk disclosures misled investors because those risks had come to fruition—were not actionable because, when stripped of mischaracterization and exaggeration, no challenged statement was false or misleading when made. *Id*. at 9-10. Generic warnings of risk may be actionable, but only where warnings state certain risks "may" occur when some of those risks have already come to fruition. *See In re Alphabet, Inc. Sec. Litig*., 1 F.4th 687, 703–04 (9th Cir. 2021). Instead, where a company acknowledges that it has already experienced the sort of challenges it warns about, as Marriott did, the risk disclosures are not actionable. *See* Order at 9-10.

Specifically, investors alleged that the "Board knew that Starwood was not . . . compliant" with certain Payment Card Industry Data Security Standards, but only warned generally of the possibility that Marriott could not comply with those standards. *Id*. at 10. However, the Court noted that this assertion was not supported by the complaint itself, which stated that Marriott's consultant found that Starwood's brand standards did not mandate Payment Card Industry compliance. Because this is what Marriott stated in its risk disclosures (that Starwood's brand standards did not mandate compliance), the statements were not misleading or false when made.

The Court affirmed dismissal, concluding that although Marriott could have provided more information to the public the federal securities laws did not require it do so.

The decision has two significant implications for companies considering how to describe their cybersecurity programs in public disclosures. First, a company should be careful about making comments concerning the strength of its cybersecurity measures, as such disclosures could potentially be considered material for securities fraud purposes. Second, a company should consider including "sweeping caveats" alongside disclosures related to its cybersecurity program in order to stave off challenges that such disclosures are misleading.

akingump.com