

**PUBLISHED**

UNITED STATES COURT OF APPEALS  
FOR THE FOURTH CIRCUIT

---

**No. 21-1802**

---

In re: MARRIOTT INTERNATIONAL, INC.

-----

CONSTRUCTION LABORERS PENSION TRUST FOR SOUTHERN  
CALIFORNIA,

Plaintiff - Appellant,

and

DENNIS MCGRATH; PETER MILLER,

Plaintiffs,

v.

MARRIOTT INTERNATIONAL, INC.; ARNE M. SORENSON; KATHLEEN  
KELLY OBERG; BAO GIANG VAL BAUDUIN; BRUCE HOFFMEISTER;  
STEPHANIE C. LINNARTZ; MARY K. BUSH; FREDERICK A. HENDERSON;  
LAWRENCE W. KELLNER; AYLWIN B. LEWIS; GEORGE MUNOZ,

Defendants - Appellees.

-----

CHAMBER OF COMMERCE OF THE UNITED STATES OF AMERICA,

Amicus Supporting Appellee.

---

Appeal from the United States District Court for the District of Maryland, at Greenbelt.  
Paul W. Grimm, District Judge. (8:19-md-02879-PWG)

---

Argued: March 10, 2022

Decided: April 21, 2022

---

Before AGEE, RUSHING, and HEYTENS, Circuit Judges.

---

Affirmed by published opinion. Judge Heytens wrote the opinion, in which Judge Agee and Judge Rushing joined.

---

**ARGUED:** Carol C. Villegas, LABATON SUCHAROW LLP, New York, New York, for Appellant. Jason J. Mendro, GIBSON, DUNN & CRUTCHER LLP, Washington, D.C., for Appellees. **ON BRIEF:** Ross M. Kamhi, David Saldamando, LABATON SUCHAROW LLP, New York, New York, for Appellant. Jeffrey S. Rosenberg, Washington, D.C., Adam H. Offenhartz, Laura K. O’Boyle, Andrei F. Malikov, GIBSON, DUNN & CRUTCHER LLP, New York, New York, for Appellees. Tara S. Morrissey, Paul Lettow, UNITED STATES CHAMBER LITIGATION CENTER, Washington, D.C.; Judson O. Littleton, Daniel J. Richardson, SULLIVAN & CROMWELL LLP, Washington, D.C., for Amicus Chamber of Commerce of the United States of America.

---

TOBY HEYTENS, Circuit Judge:

Following a major data breach targeting servers owned by Marriott International, various investors alleged that Marriott and its executives violated federal securities laws by omitting material information about data vulnerabilities in their public statements. Because the investors have not adequately alleged that any of Marriott's statements were false or misleading when made, we affirm the district court's dismissal of the complaint.

I.

In 2016, Marriott merged with Starwood Hotels and Resorts Worldwide. In doing so, "Marriott subsumed all of Starwood and its operations, including Starwood's computer systems, reservation software, and databases, as well as all the sensitive personal information in those databases." JA 578.

Two years later, Marriott learned that malware had impacted approximately 500 million guest records in the Starwood guest reservation database, resulting in the second largest data breach in history. Soon after, the Construction Laborers Pension Trust for Southern California (the investor) filed a putative class action against Marriott and nine of its officers and directors, alleging that Marriott's failure to disclose severe vulnerabilities in Starwood's IT systems rendered 73 different public statements false or misleading in violation of Section 10(b) of the Securities Exchange Act of 1934 and Securities and Exchange Commission Rule 10b-5. The investor 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, concluding that the complaint "failed to adequately allege a false or misleading statement or omission,

a strong inference of scienter, and loss causation,” which doomed the claim under Section 10(b) and Rule 10b-5 as well as the secondary liability claim. JA 1317. The investor appealed, dropping its challenge to 55 of the statements while maintaining its challenge to the other 18. We review the grant of a motion to dismiss de novo, accepting the complaint’s factual allegations as true and drawing all reasonable inferences in favor of the plaintiff. *KBC Asset Mgmt. v. DXC Tech. Co.*, 19 F.4th 601, 607 (4th Cir. 2021).

## II.

To state a claim under Sections 10(b) and 20(a) of the Securities Exchange Act of 1934 and SEC Rule 10b-5, a plaintiff must first allege a “material misrepresentation or omission by the defendant.” *Stoneridge Inv. Partners, LLC v. Scientific-Atlanta, Inc.*, 552 U.S. 148, 157 (2008); see *Yates v. Municipal Mortg. & Equity, LLC*, 744 F.3d 874, 894 n.8 (4th Cir. 2014) (“Section 20(a) liability is derivative of [Section] 10(b).”); see also 15 U.S.C. §§ 78j(b), 78t(a); 17 C.F.R. § 240.10b-5. The plaintiff must identify “a *factual* statement or omission—that is, one that is demonstrable as being true or false.” *Longman v. Food Lion, Inc.*, 197 F.3d 675, 682 (4th Cir. 1999). The challenged statement or omission must also be about something consequential—or, as the law puts it, “*material*.” *Id.* And the plaintiff must allege that the defendant either said something that is “*false*” or left something out that renders “*misleading*” the “public statements” the defendant made. *Id.*

That last point is critical to this case: Not all material omissions are actionable. Although investors would surely prefer to know everything about a company, Section 10(b) and Rule 10b-5 “do not create an affirmative duty to disclose any and all material information.” *Matrixx Initiatives, Inc. v. Siracusano*, 563 U.S. 27, 44 (2011). Rather,

“[d]isclosure is required . . . only when necessary ‘to make . . . statements made, in the light of the circumstances under which they were made, not misleading.’” *Id.* (quoting 17 C.F.R. § 240.10b-5(b)). In other words, an omission is actionable only if—absent the fact omitted—“a reasonable investor, exercising due care, would gather a false impression from a statement, which would influence an investment decision.” *Phillips v. LCI Int’l, Inc.*, 190 F.3d 609, 613 (4th Cir. 1999). As a result, “companies can control what they have to disclose” by “controlling what they say to the market.” *Matrixx Initiatives*, 563 U.S. at 45.

On appeal, the investor focuses on three categories of statements: statements about the importance of protecting customer data; privacy statements on Marriott’s website; and cybersecurity-related risk disclosures. Because the complaint failed to adequately allege that any of the challenged statements was false or rendered any of Marriott’s public statements misleading, the district court correctly held that the investor has not stated a valid claim under Section 10(b) and Rule 10b-5. For that same reason, the district court also correctly held that the investor has not stated a valid claim under Section 20(a). See *Yates*, 744 F.3d at 894 n.8.

A.

The first set of statements the investor challenges involves the importance of data protection to Marriott’s business. For example, in SEC submissions, Marriott repeatedly stated that “the integrity and protection of customer, employee, and company data is critical to us as we use such data for business decisions and to maintain operational efficiency.” JA 782, 811, 835. By “failing to disclose . . . the vulnerable state of Starwood’s IT systems,”

the investor insists, these statements “creat[ed] the misleading impression that Marriott was securing and protecting the customer data acquired from Starwood.” Investor Br. 52–53.

We are unpersuaded. The “basic problem” with the complaint on this point is that “the facts it alleges do not contradict [Marriott’s] public disclosures.” *Teachers’ Ret. Sys. of La. v. Hunter*, 477 F.3d 162, 182 (4th Cir. 2007). Indeed, the investor’s whole theory of the case turns on those statements being true—*i.e.*, that data integrity *is* “critically important to Marriott and its investors.” Investor Br. 4.<sup>1</sup>

Reiterating this basic truth is neither misleading nor creates the false impression the investor suggests. The investor relies heavily on district court decisions concluding that “statements touting the strength or quality of an important business operation are false, and thus actionable, when those operations are, in reality, deficient.” *In re Equifax Inc. Sec. Litig.*, 357 F. Supp. 3d 1189, 1220 (N.D. Ga. 2019); see Investor Br. 53, 57–58. But even assuming we agreed with those decisions (a point we need not decide), Marriott made no such representation. Instead, as the district court here explained, Marriott’s public statements about the importance of data protection did not “assign a quality to Marriott’s cybersecurity that it did not have.” JA 1361. “[I]ndeed, unlike the statements found to be

---

<sup>1</sup> Marriott’s statement that data security was “critically important” to it also amounts to little more than puffery. See *Dunn v. Borta*, 369 F.3d 421, 431 (4th Cir. 2004) (“[T]he judiciary has long distinguished between mere puffing statements utilizing opinion and exaggeration to pitch a sale, on the one hand, and factual statements that constitute fraudulent misrepresentations, on the other.”). “[P]uffery will often not be actionable” under the securities fraud laws, *Longman*, 197 F.3d at 683, and as we explain, we will not treat Marriott’s puffery any differently.

actionable in *Equifax*, Marriott made no characterization at all with respect to the quality of its cybersecurity, only that Marriott considered it important.” *Id.*

Nor could a reasonable reader of Marriott’s public statements have understood the company to be overrepresenting the extent to which it was “securing and protecting the customer data” (Investor Br. 52–53), especially when taken together with the other statements Marriott made in the same SEC filing. The reason is straightforward: Marriott’s SEC submission discloses the key risks that the investor alleges made Starwood’s systems vulnerable. The company, Marriott repeatedly warned, may “fail[] to keep pace with developments in technology”; its systems “may not be able to satisfy” the “information, security, and privacy requirements” imposed by laws and regulations; and there were risks of “significant theft, loss, or fraudulent use of” company and customer data and “[b]reaches in the security of our information systems.” See, *e.g.*, JA 784–85.

## B.

The investor’s arguments about a series of privacy statements Marriott posted on various websites fail for similar reasons. On its own website, Marriott stated that it “seek[s] to use reasonable organizational, technical and administrative measures to protect” personal data, while noting that “no data transmission or storage system can be guaranteed to be 100% secure.” JA 804, 851. Starwood’s website, in turn, said that the company “recognize[d] the importance of information security”; was “constantly reviewing and enhancing our technical, physical, and logical security rules and procedures”; and that its “web sites and servers have security measures in place to help protect your personal data.”

JA 828. At the same time, the Starwood site cautioned that “‘guaranteed security’ does not exist either on or off the Internet.” *Id.*

Again—even assuming all of the complaint’s factual allegations are true—none demonstrates that the challenged privacy statements were false or misleading. Indeed, the complaint concedes that Marriott devoted resources and took steps to strengthen the security of Starwood’s systems. And “[t]he fact that a company has suffered a security breach does not demonstrate that the company did not place significant emphasis on maintaining a high level of security.” *Equifax*, 357 F. Supp. 3d at 1221 (quotation marks omitted).

The remaining privacy statements were accompanied by such sweeping caveats that no reasonable investor could have been misled by them. For example, Marriott’s assurance that “personal data will be kept in a form which enables [us] to identify you for no longer than it is necessary for the purposes for which we collected and use your data” specifically noted that “some types of information may be stored indefinitely due to technical constraints.” JA 827. And despite high-level representations on Marriott’s website that the company “certified” its compliance with certain privacy frameworks (JA 851), Marriott’s risk disclosures to the SEC—the content actually directed to investors—specifically warned that the company’s systems “may not be able to satisfy” the “increasingly demanding” and “changing” legal and regulatory requirements. See, *e.g.*, JA 784.

### C.

We also disagree with the investor’s assertion that Marriott’s cybersecurity risk disclosures were materially misleading because they “warned of risks that had already



materialized.” Investor Br. 65–66. To be sure, “[a] generic warning of a risk will not suffice when undisclosed facts on the ground would substantially affect a reasonable investor’s calculations of probability.” *Singer v. Reali*, 883 F.3d 425, 442 (4th Cir. 2018) (quotation marks omitted). For that reason, warning of “risks that ‘could’ or ‘may’ occur” might be misleading to a reasonable investor where the defendant “knew that those risks had materialized,” but only if the risk disclosures “speak[ ] entirely of as-yet-unrealized risks and contingencies and do not alert[ ] the reader that some of these risks may already have come to fruition.” *In re Alphabet, Inc. Sec. Litig.*, 1 F.4th 687, 703–04 (9th Cir. 2021) (quotation marks omitted). In contrast, a risk disclosure’s forward-looking statements do not “constitute[ ] misleading omissions about current or past challenges” when “the disclosure also acknowledge[s] that the company had already experienced the sort of challenges that it would have to overcome in order to achieve its stated objective.” *Id.* (quotation marks and citation omitted).<sup>2</sup>

The investor argues that Marriott twice warned generally about events that could occur when it knew those events *had in fact* already occurred. Although we construe the complaint’s allegations about the underlying facts in the light most favorable to the investor, we must first “strip[ ] . . . allegations of mischaracterizations and exaggeration, [and] focus on whether the exact statement in its true context constitutes a material

---

<sup>2</sup> Such risk disclosures generally also lack materiality because “[t]hey are not meant to educate investors on what harms are currently affecting the company,” so “a reasonable investor would be unlikely to infer anything” from them about the company’s current state of affairs. *Bondali v. Yum! Brands, Inc.*, 620 Fed. Appx. 483, 491 (6th Cir. 2015).

representation.” *Phillips*, 190 F.3d at 617. And, when we do so, we conclude the investor has failed to identify any statement that was false or misleading when made.

For example, the investor takes issue with Marriott’s warning that its “systems . . . may not be able to satisfy” the “changing requirements” of “the payment card industry” (see, *e.g.*, JA 784), arguing that Marriott “warned only generally of the possibility that Marriott would not be able to comply with the requirements of the payment card industry” after “the Board knew that Starwood was not . . . compliant” with the Payment Card Industry Data Security Standards (PCI DSS). Investor Br. 66–67. But the investor’s assertion that Marriott and its executives were “aware that they were not satisfying [PCI DSS] requirements” (Investor Br. 67) is not supported by the investor’s own allegations. According to the complaint, Marriott’s consultant reported that Starwood’s “[b]rand standards *did not mandate* PCI compliance,” not that Starwood’s systems were, in fact, not compliant. JA 705 (emphasis added). At most, the consultant’s report informed Marriott only that Starwood’s systems might not satisfy PCI DSS requirements—which is what Marriott stated in its risk disclosures.

The investor also argues that, despite having “actual knowledge of the Data Breach,” Marriott’s SEC disclosures from November 6, 2018 “warned generally of the risk that Marriott could face disruptive cyber security incidents,” such as “[e]fforts to hack or circumvent security measures” and “attempts to affect the integrity of our data.” Investor Br. 67 (citing JA 859–60). But Marriott’s “disclosure also acknowledged that the company had already experienced the sort of challenges” being discussed. *Alphabet*, 1 F.4th at 703–04 (quotation marks and citation omitted). Specifically, after learning of the breach,

Marriott updated its disclosure to state: “[W]e have experienced cyber-attacks, attempts to disrupt access to our systems and data, and attempts to affect the integrity of our data, and the frequency and sophistication of such efforts could continue to increase.” JA 860. This admission ensured that forward-looking warnings did not “constitute[] misleading omissions about current or past challenges.” *Alphabet*, 1 F.4th at 703–04 (quotation marks omitted).

\* \* \*

Marriott certainly could have provided more information to the public about its experience with or vulnerability to cyberattacks, but the federal securities laws did not require it to do so. Indeed, the SEC advises companies against “mak[ing] detailed disclosures that could compromise [their] cybersecurity efforts—for example, by providing a ‘roadmap’ for those who seek to penetrate a company’s security protections.” SEC Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8166, 8169 (Feb. 26, 2018). Even as alleged here, Marriott provided sufficient information to ensure its statements were neither false nor misleading. The judgment of the district court is therefore

*AFFIRMED.*