

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MARYLAND**

**IN RE: MARRIOTT INTERNATIONAL,  
INC., CUSTOMER DATA SECURITY  
BREACH LITIGATION** \* \* **MDL No. 19-md-2879**

## **SECURITIES ACTIONS**

## **MEMORANDUM OPINION**

This case involves the consolidated class action complaint filed by Plaintiff Construction Laborers Pension Trust for Southern California against Defendants Marriott International, Inc. and nine of its corporate officers and directors for violations of the securities laws related to a data breach of the Marriot-owned Starwood Hotels and Resorts, Inc.<sup>1</sup> It is part of the Multidistrict Litigation (“MDL”) pending before me concerning the data breach. Plaintiff alleges that Defendants made 73 false or misleading statements or omissions in violation of Section 10(b) of the Securities Exchange Act of 1934 (“Exchange Act”) and SEC Rule 10b-5 promulgated thereunder (“Rule 10b-5”). Plaintiff also brings a claim for secondary liability under Exchange Act Section 20(a). Defendants moved to dismiss under the Private Securities Litigation Reform Act of 1995 (“PSLRA”), and Rules 12(b)(6) and 9(b) of the Federal Rules of Civil Procedure.<sup>2</sup> As explained below, Defendants’ motion to dismiss is granted because Plaintiff has failed to adequately allege a false or misleading statement or omission, a strong inference of scienter, and loss causation. Plaintiff’s claims are dismissed with prejudice.

<sup>1</sup> Third Amended Consolidated Complaint (“Complaint”), ECF No. 609. References to “¶ \_\_” throughout are citations to the Complaint.

<sup>2</sup> The motion is fully briefed. See ECF Nos. 647, 669, 679, 690, 711, 717. A hearing is not necessary. See Loc. R. 105.6 (D. Md. 2018).

## BACKGROUND

Plaintiff Construction Laborers Pension Trust for Southern California is a multi-employer pension plan that alleges it acquired thousands of shares of Marriott's securities and incurred substantial losses caused by allegedly false and misleading statements and omissions related to the data breach. ¶ 49. Plaintiff brings claims on behalf of itself and all persons and entities who purchased or otherwise acquired Marriott's publicly traded securities from November 16, 2015 to November 29, 2018 (the "Class Period") and who were damaged as a result of the allegedly false and misleading statements and omissions related to the data breach. ¶ 1.

Plaintiff names as defendants Marriott, along with nine of its corporate officers and board members (collectively, the "Individual Defendants"). Marriott is a worldwide operator, franchisor, and licensor of hotel, residential, and timeshare properties that is incorporated in Delaware and headquartered in Bethesda, Maryland. ¶ 50. Four of the Individual Defendants are Marriott corporate officers: Mr. Arne Sorenson, Marriott's Chief Executive Officer since 2012 and a board member since 2011 until his recent death in 2021; Ms. Kathleen Oberg, Marriott's Chief Financial Officer since 2016; Mr. Bao Giang Val Bauduin, Marriott's Chief Accounting Officer since 2014; and Mr. Bruce Hoffmeister, Marriott's Chief Information Officer since 2011, though Defendants state that he has recently retired. ¶¶ 51–54. The five remaining Individual Defendants are current or former members of Marriott's Board of Directors and Audit Committee. At the start of the Class Period, the Audit Committee had three members: Defendants Ms. Mary Bush, Mr. Frederick Henderson, and Mr. Lawrence Kellner. ¶ 55. On September 23, 2016, the Audit Committee expanded to four members: Defendants Ms. Mary Bush, Mr. Frederick Henderson, Mr. George Muñoz, and Mr. Aylwin Lewis. *Id.*

Plaintiff's allegations are centered on Marriott's acquisition of Starwood Hotels and Resorts Worldwide a subsequently identified breach of Starwood's guest reservations database.

On November 16, 2015, Marriott announced that it would acquire Starwood. ¶ 122. Before the merger closed, Marriott conducted due diligence on Starwood, including on its IT systems. ¶ 136. Marriott continually updated investors on the progress of the Starwood merger in its SEC filings and other public statements. These statements form the basis of Plaintiff's claims and are discussed in detail below. The merger closed on September 23, 2016, at which point Marriott subsumed Starwood's assets, liabilities, and operations. ¶ 50.

On September 7, 2018, IBM Guardium, a security tool used by Marriott, generated an alert that an unknown user had run a query in the Starwood guest reservation database. ¶ 32. Accenture, a third-party IT contractor that was tasked with running the Starwood guest reservation database, alerted Marriott the following day. *Id.* Marriott brought in third-party investigator Crowdstrike two days later. *Id.* On September 17, 2018, Crowdstrike found malware that could be used to access or monitor a computer. ¶ 256. Mr. Sorenson informed the Board the next day. *Id.* The investigation continued and on November 13, 2018, Crowdstrike discovered that two encrypted files had been deleted. ¶ 259. On November 19, 2018, Crowdstrike discovered that the files contained customers' personal information. *Id.* On that day, Marriott began preparing to notify affected guests, and on November 30, 2018, Marriott publicly announced the data breach. *Id.*; ¶ 262.

Following the announcement of the data breach, Marriott contracted Verizon to conduct a forensic investigation of the incident. ¶ 331. Verizon conducted the investigation and authored a report on its findings, known as the Payment Card Industry Forensic Investigator ("PFI") Report. The PFI Report found that Starwood's systems were compromised for a period of more than four years, starting as early as July 28, 2014. ¶ 331. Therefore, the data breach was occurring for approximately two years before and after Marriott's acquisition of Starwood. The PFI Report's

findings include that Starwood's system (1) allowed for insecure remote access; (2) lacked or had insufficient access/query and firewall logging; (3) lacked monitoring and logging of remote access; and (4) Starwood inadvertently stored payment account numbers on systems and in databases that were not designated for the storage of payment account numbers. ¶ 335. The data breach compromised the personal information of more than 380 million people, including name, payment card data, passport information, traveling companions, and home address. ¶ 618. The scope of the breach gives it the inauspicious designation of the second largest data breach in history. *Id.*

On December 1, 2018, the day after the data breach was announced, a litigant filed the first securities class action lawsuit against Marriott. *See McGrath v. Marriott Int'l, Inc.*, No. 18-6845 (E.D.N.Y. Dec. 1, 2018). The Judicial Panel on Multidistrict Litigation transferred that lawsuit to this Court. ECF No. 1. I consolidated the securities class actions and appointed Construction Laborers Pension Trust for Southern California and its counsel as lead plaintiff and counsel. *See* ECF No. 238. Now on its third amended consolidated complaint, Plaintiff alleges two counts. The first count is brought under Section 10(b) of the Exchange Act and Rule 10b-5 for alleged false and misleading statements and omissions. ¶¶ 656–63. The second count is for secondary liability for control persons under Section 20(a) of the Exchange Act. ¶¶ 664–72. Pending is Defendants' motion to dismiss under the PSLRA and Rules 12(b)(6) and 9(b) of the Federal Rules of Civil Procedure. ECF No. 647.

### **STANDARD OF REVIEW**

Federal Rule of Civil Procedure 12(b)(6) provides for the dismissal of a complaint for "failure to state a claim upon which relief can be granted." This rule's purpose "is to test the sufficiency of a complaint and not to resolve contests surrounding the facts, the merits of a claim, or the applicability of defenses." *Presley v. City of Charlottesville*, 464 F.3d 480, 483 (4th Cir.

2006). A complaint must contain “a short and plain statement of the claim showing that the pleader is entitled to relief.” Fed. R. Civ. P. 8(a)(2). Specifically, plaintiff must establish “facial plausibility” by pleading “factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). But “[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice.” *Id.* Well-pleaded facts as alleged in the complaint are accepted as true. *See Aziz v. Alcolac*, 658 F.3d 388, 390 (4th Cir. 2011). Factual allegations must be construed “in the light most favorable to [the] plaintiff.” *Adcock v. Freightliner LLC*, 550 F.3d 369, 374 (4th Cir. 2008) (quoting *Battlefield Builders, Inc. v. Swango*, 743 F.2d 1060, 1062 (4th Cir. 1984)).

Where, as here, the allegations in a complaint sound in fraud, the plaintiff also must satisfy the heightened pleading requirements of Federal Rule of Civil Procedure 9(b) by “stat[ing] with particularity the circumstances constituting fraud.” This requires that the plaintiff allege “the time, place, and contents of the false representations, as well as the identity of the person making the misrepresentation and what he obtained thereby.” *Harrison v. Westinghouse Savannah River Co.*, 176 F.3d 776, 784 (4th Cir. 1999) (internal quotation marks omitted).

Because Plaintiff alleges securities fraud under Exchange Act Section 10(b) and SEC Rule 10b-5, he must also face the higher burden imposed by Congress in the PSLRA, 15 U.S.C. § 78u-4. For each alleged material misrepresentation or omission, “the complaint shall specify each statement alleged to have been misleading, the reason or reasons why the statement is misleading, and, if an allegation regarding the statement or omission is made on information and belief, the complaint shall state with particularity all facts on which that belief is formed.” 15 U.S.C. § 78u-4(b)(1). In addition, for each alleged misrepresentation or omission, the complaint must “state

with particularity facts giving rise to a strong inference that the defendant acted with the required state of mind.” 15 U.S.C. § 78u-4(b)(2). If a complaint fails to meet these requirements, it must be dismissed. 15 U.S.C. § 78u-4(b)(3)(A).

## DISCUSSION

### **I. Securities Fraud Under Exchange Act 10(b) and SEC Rule 10b-5**

In Count I, Plaintiff alleges a violation of Section 10(b) of the Exchange Act and Rule 10b-5. ¶¶ 656–63. “The purpose of the Exchange Act and its accompanying regulations is to ensure that companies disclose the information necessary for investors to make informed investment decisions.” *Yates v. Mun. Mortg. & Equity, LLC*, 744 F.3d 874, 884 (4th Cir. 2014). Section 10(b) of the Exchange Act prohibits the use of “any manipulative or deceptive device or contrivance” in connection with the sale of a security in violation of SEC rules. 15 U.S.C. § 78j(b). Rule 10b-5 makes it unlawful, in connection with the sale of a security:

- (a) To employ any device, scheme, or artifice to defraud,
- (b) To make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading, or
- (c) To engage in any act, practice, or course of business which operates or would operate as a fraud or deceit upon any person.

17 C.F.R. § 240.10b-5. This Rule grants purchasers of a security an implied right of action to bring a claim for violations of Section 10(b) of the Exchange Act. *See Stoneridge Inv. Partners v. Scientific–Atlanta, Inc.*, 552 U.S. 148, 157 (2008); *Yates v. Mun. Mortg. & Equity, LLC*, 744 F.3d at 884.

To prevail in a § 10(b) action, a private plaintiff must prove six elements: “(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.” *Stoneridge Inv.*

*Partners v. Scientific–Atlanta, Inc.*, 552 U.S. at 157; *see also Yates v. Mun. Mortg. & Equity, LLC*, 744 F.3d at 884. Defendants argue that Plaintiff fails to adequately allege a material misrepresentation or omission, scienter, and loss causation. Defendants also argue that there is no connection between Marriott’s privacy statements and the purchase and sale of a security.

#### **a. Material Misrepresentations and Omissions**

Plaintiff alleges that 73 statements made by Defendants during the class period were material misrepresentations or omissions. To be actionable, the challenged statements must meet three requirements. First, the alleged misrepresentation or omission must be “*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) (citing *Virginia Bankshares, Inc. v. Sandberg*, 501 U.S. 1083, 1091–96 (1991)). Second, the statement itself must be false or the omission must render the statement misleading. *Id.*; 17 C.F.R. § 240.10b–5. Finally, the misrepresentation or omission must be material. *Id.* “Materiality is an objective concept, ‘involving the significance of an omitted or misrepresented fact to a reasonable investor.’” *Id.* at 682–83 (quoting *Gasner v. Bd. of Sup’rs of the Cty. of Dinwiddie, Va.*, 103 F.3d 351, 356 (4th Cir. 1996)). A statement or omission of fact is material “if there is a substantial likelihood that a reasonable purchaser or seller of a security (1) would consider the fact important in deciding whether to buy or sell the security or (2) would have viewed the total mix of information made available to be significantly altered by disclosure of the fact.” *Id.* at 683 (citing *Basic Inc. v. Levinson*, 485 U.S. 224, 231–32 (1988); *TSC Indus., Inc. v. Northway, Inc.*, 426 U.S. 438, 448–49 (1976); *Gasner*, 103 F.3d at 356)).

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). Instead, “[d]isclosure is required under these provisions only when necessary ‘to make . . . statements made,

in the light of the circumstances under which they were made, not misleading.’’ *Id.* (quoting 17 CFR § 240.10b-5(b)). ‘‘Even with respect to information that a reasonable investor might consider material, companies can control what they have to disclose under these provisions by controlling what they say to the market.’’ *Id.* at 45; *see also Basic Inc. v. Levinson*, 485 U.S. 224, 239 n.17 (‘‘Silence, absent a duty to disclose, is not misleading under Rule 10b-5.’’).

Statements of opinion or puffery generally are not actionable. *Id.* But in particular contexts, a statement of opinion or puffery can be actionable when it is both factual and material. *Id.* As the Fourth Circuit explained:

[F]or example, a CEO's expression of ‘‘comfort’’ with a financial analyst's prediction of his company's future earnings was held not to be factual in that, as a future projection, it was not capable of being proved false. *See Malone v. Microdyne Corp.*, 26 F.3d 471, 479–80 (4th Cir. 1994); *see also Raab v. General Physics Corp.*, 4 F.3d 286, 289 (4th Cir. 1993) (holding similar statement predicting future growth not material because ‘‘the market price of a share is not inflated by vague statements predicting growth’’). On the other hand, the Supreme Court has held that an opinion by board members to minority stockholders that the stock price of \$42 for the purchase of their shares was a ‘‘high value’’ and represented a ‘‘fair’’ transaction could be both factual and material. *See Virginia Bankshares*, 501 U.S. at 1090–93. In *Virginia Bankshares*, the Court noted that the opinions could be false and factual if the directors did not believe what they said they believed and proof could be had ‘‘through the orthodox evidentiary process.’’ *Id.* at 1093.

*Longman v. Food Lion, Inc.*, 197 F.3d 675 at 683.

In their briefs, the parties grouped the alleged statements of material misrepresentation and omission into various categories. I use the same categorizations for purposes of this discussion. Each alleged statement, and its category or categories, is also summarized in Appendix A.

For each allegedly false or misleading statement or omission in the Complaint, Plaintiff repeats the same core allegations for why the statement was false or misleading, with some additions over time. These core allegations are that at the time the statements were made, Starwood's IT systems were severely vulnerable, including because (1) the systems were using an outdated Oracle application portal that could not be updated or patched; (2) the legacy Starwood

system allowed for insecure remote access; (3) only a fraction of Starwood's firewall activity was being logged, so nobody could adequately monitor for attacks; (4) the legacy Starwood system lacked monitoring and logging of remote access, meaning that there was no record of who was remotely accessing the systems; (5) not all database queries were being logged, so nobody could see if a hacker was accessing Starwood's valuable data without permission; and (6) payment account numbers were being stored without encryption. *See, e.g., ¶445.* In other words, Plaintiff's allegations focus on alleged deficiencies in Starwood's systems. Plaintiff attempts to turn these alleged deficiencies into a Section 10(b) claim for false statements by alleging that an adequate due diligence process would have revealed these alleged deficiencies and that Defendants knew or were severely reckless in not knowing that they were making false or misleading statements regarding Marriott's due diligence, integration, risks, and prospects.

In addition, for each alleged false or misleading statement or omission, Plaintiff alleges that the statement or omission (1) gave investors a false impression that Marriott had undertaken sufficient due diligence; (2) gave investors a false impression that Marriott made adequate preparations and dedicated adequate resources to cybersecurity; and (3) gave investors the false sense that Marriott's prior acquisition experience was relevant. *See, e.g., id.* Plaintiff also alleges that Marriott's board was aware of the risks that cybersecurity posed to the company but ignored red flags including (1) Starwood's known cybersecurity issues; (2) breaches of Marriott's competitors in the hospitality industry; and (3) other significant data breaches. *See, e.g., id.*

Finally, Plaintiff alleges that for each statement, Defendants failed to share Starwood's alleged security deficiencies with the market. *See, e.g., id.*

Plaintiff copy and pastes this same set of allegations to challenge statements in Marriott's periodic SEC filings and SEC filings about the Starwood acquisition in addition to other public

statements during the Class Period. But an examination of the statements shows that Plaintiff's cookie-cutter approach misses the mark.

### i. Statements About Due Diligence and Integration

Plaintiff alleges that Defendants made material misrepresentations and omissions regarding their due diligence and integration of Starwood during the merger process. *See ¶¶ 442–44, 448–49, 452, 464–67, 470, 474, 476, 478, 480, 489, 501, 526, 543, 545, 574, 577–78, 580, 582.* Many of these statements appeared in Marriott's public SEC filings. For example:

Marriott's Board, in arriving at its decision to recommend the Merger, “*consulted with Marriott's senior management, legal advisors, financial advisors, and other advisors,*” and later stated that the Board “*reviewed a significant amount of information.*” Additionally, those documents informed the market that “*both Marriott's and Starwood's strong track records in merger integration*” supported voting in favor of the Merger.<sup>3</sup>

¶ 448 (December 22, 2015, Form S-4 Registration Statement; January 27, 2016, First Amendment to the Registration Statement; February 16, 2016, Second Amendment to the Registration Statement; February 17, 2016, Prospectus).

We were thrilled to close the acquisition of Starwood in late September. We are enthusiastically engaged in welcoming Starwood's associates around the world into the Marriott family and *are working diligently on integrating the companies* and realizing revenue and cost synergies as quickly as possible.

¶ 501 (November 7, 2016, Form 8-K). Other statements were made during conference calls with investors, on social media, or in press releases. For example:

We've talk [sic] a little bit about cost synergies. This is now on page 10 for those of you who are following along. *We have been working intensely since we announced this deal in November to prepare for integration and of course, to understand each other's organizations and structures and start to think about how to meld those into one organization.*

¶ 466 (March 21, 2016, Conference Call to Discuss Amended Merger Agreement).

---

<sup>3</sup> Text that is bolded and italicized throughout is original to the Complaint, and signifies the portion of a statement that Plaintiff alleges is false or misleading. *See ¶ 202 n.173.*

Since we announced the merger in November 2015, our integration teams have met on average multiple times a week across disciplines. *As a result of our extensive due diligence and joint integration planning, we are now even more confident in the potential of cost savings of this transaction.*

¶ 467 (March 21, 2016, LinkedIn Statement).

Analyst

Good morning, everyone. A quick question on cost synergies. Just wondering if you can provide a little more elaboration on -- the previous estimate was \$200 million, it went to \$250 million, that is. What was included in the incremental \$50 million, and is there any reason to believe that with more information there could be more to come on that front?

Sorenson

So Tom thought we could do \$250 million from the moment we announced a deal. And he knows the cost structure at Starwood, obviously dramatically better than we do. And I guess in a way we just were acknowledging that he was right. For us, we want to take it a step at a time and we hadn't, when we announced the deal, really done any organizational diligence, if you will. *We've done financial diligence and tried to understand the assets and the balance sheet and those sorts of things.*

*But in the four months we've had following, we've had -- I think one of our team, the Starwood integration [lead] counted 150-ish meetings between Marriott and Starwood people in various disciplines or various regions around the world, where they are getting to know each other, where they are getting to know the organizations, where they are starting to think about what the combined organization looks like from a staffing level going forward.* And all of that has given us greater confidence that the \$250 million number is achievable. We don't have another number to hang out for you as further upside from that.

¶ 478 (April 1, 2016, Marriott and Starwood M&A Conference Call).

Siegel

It's been more than a year since Marriott International merged with Starwood. From your perspective, how's the integration process going?

Hoffmeister

Whenever two large companies come together, you have to determine what processes, systems and tools to use. *We're going through the process of bringing our systems together to get the best of both worlds wherever possible.* It's very exciting. We have a lot going on, and a lot of work ahead still, but it's a very exciting time.

\*\*\*

Siegel

At the Download conference, you mentioned that when you learned of the Starwood merger, as CIO you looked for advice from other CIOs. Can you elaborate on that?

Hoffmeister

\*\*\*

Two themes emerged. The first was quite simply to “just adopt and go.” Choose your systems and just go with them; you’re not going to please everyone. ***We did a thorough analysis of the systems before we made our decision***, but we didn’t dwell on it, we just made a decision.

¶ 544 (January 12, 2018, Hoffmeister Interview). To summarize, the focus of these allegedly false or misleading statements is that Marriott was working “diligently,” “thoroughly,” and “intensely” to integrate the companies, reviewed “a significant amount of information,” and completed a “thorough analysis” and “extensive due diligence.” Plaintiff alleges that these statements are material misrepresentations because at the time they were made, Starwood’s IT systems were severely vulnerable, which an adequate due diligence process would have uncovered, and because they gave investors the false impression that Marriott had undertaken sufficient due diligence, that Marriott had made adequate preparations and dedicated adequate resources to cybersecurity, and that Marriott’s prior acquisition experience was relevant to the due diligence and integration processes. *See, e.g.*, ¶¶ 450–51.

Plaintiff’s claims regarding the due diligence and integration statements fail for several reasons. To begin with, what stands out is that none of the statements alleged to be material misrepresentations were regarding cybersecurity due diligence or integration in particular. All but one were made in the context of the due diligence and integration of two companies as a whole – companies with thousands of properties and employees around the globe. When one international corporation investigates whether to merge with another, the decision requires analysis of myriad aspects of the operations of each: the competence and experience of senior management; balance

sheet and financial condition; earnings, debt load and profitability; business operations practices; personnel and employee practices and culture; compatibility of products offered—the list is extensive. Analysis of the statements made about the merger process must fairly consider the context in which the statements were made, and representations made regarding the entirety of the complex overall process are a far cry from specific representations about one detailed aspect of the much larger whole. The Complaint contains no allegations to support the inference that Marriott was not conducting extensive due diligence or spending time to integrate the companies generally as Marriott’s statements claim. Indeed, the Complaint itself includes the statement that by April 2016, Marriott and Starwood had approximately 150 integration meetings. ¶ 478 (April 1, 2016, Marriott and Starwood M&A Conference Call).

The remaining statement that was not about due diligence and integration of the companies as a whole is the statement from Mr. Hoffmeister, Marriott’s Chief Information Officer, that Marriott did a “thorough analysis” of Marriott and Starwood’s systems before deciding which to keep. ¶ 544. But here again, the Complaint contains no allegations that Mr. Hoffmeister made representations about cybersecurity that would render his statement false or misleading. And according to the Complaint, one of Plaintiff’s Confidential Witnesses, a Marriott Senior Director responsible for IT integration, stated that he attended “many due diligence meetings prior to and during the sale,” that “the IT leadership team sat down and went through every Starwood system before the acquisition,” and that “the due diligence process was extremely detailed.” ¶ 175. Therefore, Plaintiff’s allegations actually support the *truth* of Mr. Hoffmeister’s statement.

Plaintiff argues that the alleged due diligence and integration statements “are actionable because they created a misleading impression that Marriott was working hard to evaluate Starwood’s systems and that there were no issues that would impede the Merger or successful

integration.” Pl. Opp. at 29. For the reasons stated above, the allegations in the Complaint do not support the inference that Marriott did not do something that it stated it was doing regarding its due diligence and integration planning. And Plaintiff’s argument that Defendants’ statements gave the misleading impression that there were “no issues that would impede the merger” has no basis in the Complaint or common sense. “Working hard” on due diligence and integration does not mean that there would be no issues, and Plaintiff provides no factual allegations to support the proposition that a reasonable investor would believe otherwise. Furthermore, as discussed below, Marriott included risk factor disclosures in its SEC filings that warned of a multitude of reasons why the merger may not be successful.

Plaintiff also argues that a finding from the European Union Information Commissioner’s Office that Marriott “failed to undertake sufficient due diligence” supports the falsity of the due diligence statements. Pl. Opp. at 29; ¶ 45. This preliminary finding by the EU Commissioner that was made after the fact does not make Marriott’s alleged statements regarding due diligence and integration false at the time they were made. “Quite simply, Plaintiffs do not get the benefit of 20/20 hindsight.” *In re Under Armour Sec. Litig.*, 342 F. Supp. 3d 658, 677 (D. Md. 2018).

Finally, Plaintiff argues that Defendants’ statements regarding due diligence and integration that were made after they allegedly had actual knowledge of the data breach are false and misleading by virtue of that knowledge. First, Plaintiff points to an interview with Mr. Sorenson on September 25, 2018 at the Salesforce “The Future of Travel & Hospitality” event:

[Interviewer]: So what would you say has been your biggest bet when it comes to technology?

Sorenson: Well, um, that’s a good question. I think the, uh, we spend a lot of money on technology. We’re spending hundreds of millions of dollars a year. *Uh, it is mostly about investing in the loyalty and reservations platform. Uh, they’re big bets but they are not risky bets . . .*

*I think the, uh, biggest bet that sort of has some risk in it . . . was our acquisition of Starwood a couple of years ago . . . \$13 billion dollars, biggest deal by a lot that Marriott has ever done. We were a \$20 billion company when we bought them so, you know, it's risking a fair amount of the Company.* And while it isn't at its core maybe a technology bet, it was a bet on the loyalty program. We said if we can bring these two companies together and have a bigger ecosystem for our customers, and they are really our customers, then we can say to them, "why would you stay anywhere else?" that would be a good thing.

[Interviewer]: You mentioned risk, what would be some of the riskier elements of technology? . . .

Sorenson: . . . You've got two examples that I'd use today. *One is the regulatory one. So we are increasingly living in a world in which data will be required to be maintained in the country of residence of your customer. GDPR in Europe is probably the most profound, China heading the same way, California of course passed a law last year. All of this is going to have some impact on where we can keep the information we have about you. And to some extent how we mine it. Can we mine it through pure anonymous tools . . . so that's an area of risks.*

¶ 574. Plaintiff alleges that this statement was false and misleading for the same reasons as discussed above, and because it was made after Mr. Sorenson and the Audit Committee Defendants had actual knowledge of the data breach.

However, Plaintiff's own allegations show that Mr. Sorenson did not know the full scope of the data breach or that customer information was compromised at the time of this interview. The Salesforce interview took place on September 25, 2019. *Id.* Plaintiff alleges that on September 7, 2018, the IBM Guardium database alert tool discovered the data breach. ¶ 255. On September 10, 2018, Marriot brought in a third-party investigator, Crowdstrike, to perform a review of the hacked systems. *Id.* By September 17, 2018, Crowdstrike determined that attackers had installed webshells, VPN tools, and malware on Starwood's systems, including a Remote Access Trojan ("RAT") – a program that allows attackers to access, surveil, and gain control over a computer. ¶ 255. The Board was notified of this information by September 18, 2018. *Id.* It was not until November 19, 2018 that Marriott learned that encrypted files containing guests'

personal information were removed. ¶ 259. Thus, Plaintiff's allegations show that Mr. Sorenson was aware that a cyber-attack had occurred before the September 25, 2018 interview, but not the extent of the attack or that customer information had been compromised, and at that time the investigation into the data breach was ongoing. These allegations do not support the inference that Mr. Sorenson made a false or misleading statement when discussing the size of the Starwood acquisition and regulatory regimes regarding where data is kept, such as the EU's General Data Protection Regulation ("GDPR"), as risks. Plaintiff fails to allege facts to show that a reasonable investor would be misled by these statements. Because they are not misleading, Mr. Sorenson was not required to disclose more under the securities laws, including in regards to Marriott's ongoing investigation in the data breach. *See Matrixx Initiatives, Inc. v. Siracusano*, 563 U.S. at 44–45 (Section 10(b) and Rule 10b-5 "do not create an affirmative duty to disclose any and all material information."); *Basic Inc. v. Levinson*, 485 U.S. at 239 n.17 ("Silence, absent a duty to disclose, is not misleading under Rule 10b-5.").

Next, Plaintiff cites two statements by Mr. Sorenson in an October 10, 2018 interview at the Skift Global Forum with Skift's Senior Hospitality Editor Deanna Ting. Ms. Ting asked Mr. Sorenson whether there were "any disappointments along the way" regarding the merger, and Mr. Sorenson stated, "*There has never been a moment of regret. . . . Have there been disappointments? Of course, but there have also been positive surprises. And I think on balance there have been more positive surprises than negative ones.*" ¶ 577. Ms. Ting also asked Mr. Sorenson about updates to Marriott's reservation platform:

Ms. Ting: Speaking of software, reservations systems, I sort of feel like your reservations platform, is overdue for an overhaul. How are you planning to update it or have you already updated it?

Mr. Sorenson: *Well we are, uh, again, this is a little bit in the context of the merger of Starwood and Marriott, uh right now in waves, we are putting all of the*

***Starwood hotels on the Marriott system. Uh, that will be done at the end of the year, uh then stabilized. We do have a new res platform that's rolling out this year . . .***

¶ 578. Plaintiff alleges these statements were false and misleading for the same reasons as the statements above. ¶ 579.

As discussed above, at the time that these statements were made – October 10, 2018 – Plaintiff’s allegations show that Mr. Sorenson was aware that a data breach occurred but not the extent of the data breach or that customer information was compromised, and that the investigation was ongoing. Plaintiff fails to allege facts to show that Mr. Sorenson’s statements in the Skift interview were false or misleading. Mr. Sorenson stated that in his view there were not any moments of regret, but there have been disappointments and positive surprises. Plaintiff alleges no facts to suggest that a reasonable investor would be misled by this statement into thinking Mr. Sorenson was making a specific representation about data security. Mr. Sorenson had no obligation to disclose the ongoing investigation into the data breach when discussing updates to the integrated reservation system. In addition, Mr. Sorenson’s statement that there were no moments of regret but positive surprises and disappointments is a statement of opinion that falls outside of the scope of Section 10(b) and Rule 10b-5. *See Raab v. Gen. Physics Corp.*, 4 F.3d 286, 289–90 (4th Cir. 1993); *see also* Section I.a.ii *infra*.

Plaintiff next cites an October 20, 2018 article from the New York Times, quoting an interview that Mr. David Flueck gave to the Richmond Times Dispatch:

In an article in the New York Times titled Marriott’s Merger of Hotel Rewards Programs Tests Members’ Loyalty, Marriott’s Senior VP of Global Loyalty David Flueck gave an interview to the Richmond Times Dispatch. In that article, Mr. Flueck “***described the merger as 99.9 percent successful***, though he acknowledged that it still left millions of customer records in limbo, some for weeks before they were resolved.”

¶ 580. Mr. Flueck is not a defendant in this case. Plaintiff does not allege that he was a member of Marriott's Board, that he had any discussions with Marriott's Board or anyone else regarding the data breach (the investigation of which was still ongoing and had yet to uncover that customer information was taken), or that he had any other knowledge of the data breach. Therefore, Plaintiff fails to provide any allegations that Mr. Flueck believed this statement to be false at the time it was made. Further, this statement that the merger was "99.9 percent successful" is statement of puffery and opinion that is not actionable.

Finally, Plaintiff alleges that Marriott's statement in its November 5, 2018 Form 8-K that "*We are in the home stretch on integrating the companies and are pleased with the results*" was a material misrepresentation. ¶ 582. Plaintiff alleges that this statement was false and misleading for the same reasons as the statements above. ¶ 583. And, like the statements above, this statement was made while the investigation into the data breach was ongoing but before Defendants knew that customer information was compromised. This statement is not specific to cybersecurity, and Plaintiff fails to allege any facts that show Marriott was not in the "home stretch" of integrating the companies as a whole or that Marriott was not "pleased" with the results at the time. In addition, the statement that Marriott was pleased with the results is another statement of puffery and opinion that is not actionable.

Because Plaintiff fails to allege facts to plausibly show that that any of these statements regarding due diligence and integration were false or misleading, it has also failed, as a matter of law, to adequately allege that Defendants made an actionable omission. *See Matrixx Initiatives, Inc. v. Siracusano*, 563 U.S. at 44 ("Disclosure is required under [Section 10(b) and Rule 10b-5] only when necessary 'to make . . . statements made, in the light of the circumstances under which they were made, not misleading.'") (quoting 17 CFR § 240.10b-5(b)).

## ii. Purported Statements of Optimism

Plaintiff alleges that statements that contain purported statements of optimism are material misrepresentations. ¶¶ 449, 452, 458, 465, 470, 474, 483, 489, 492, 503, 513, 519, 528, 537, 551, 557, 564, 585. Portions of these statements fall into the categories of “due diligence and integration,” discussed above in section I.a.i or “risk factor disclosures,” discussed below in section I.a.iii. This section deals with the portions of these statements regarding Defendants’ positive outlook on the merger. Some of these statements appear in SEC filings. For example:

*Given Marriott’s Board’s knowledge of Marriott’s business, operations, financial condition, earnings and prospects and Marriott’s Board’s knowledge of Starwood’s business, operations, financial condition, earnings and prospects, taking into account Starwood’s publicly filed information and the results of Marriott’s due diligence review of Starwood, the prospects for the combined company are favorable.*

¶ 449 (December 22, 2015, Form S-4 Registration Statement; January 27, 2016, First Amendment to the Registration Statement; February 16, 2016, Second Amendment to the Registration Statement; February 17, 2016, Prospectus). Others were made in press releases or conference calls with investors. For example:

*In the further diligence we have completed in last five months, we have become even more convinced of the tremendous opportunity presented by this merger. That confidence is reflected in our higher offer. We now believe there are more cost synergies than we estimated in November.*

¶ 465 (March 21, 2016, Conference Call to Discuss Amended Merger Agreement).

*After five months of extensive due diligence and joint integration planning with Starwood, including a careful analysis of the brand architecture and future development prospects, we are even more excited about the power of the combined companies and the upside growth opportunities.*

¶ 474 (March 21, 2016, Form 8-K Press Release).

To summarize, the focus of these allegations is that Defendants stated the prospects for the merger were “favorable,” and that they were “excited” and “optimistic” about the “tremendous opportunity” the merger presented.

Plaintiff pleads the same allegations described above for why these statements are false or misleading. *See, e.g.*, ¶ 450–51. The thrust of the allegations, as applied to these statements, is that Defendants knew or were severely reckless in not knowing Starwood’s cybersecurity deficiencies, and therefore their statements of optimism regarding the merger contained material misrepresentations or omissions.

Plaintiff’s allegations regarding the statements of optimism fail for several reasons. First, these statements of optimism constitute “puffing” statements that are not actionable. *See Raab v. Gen. Physics Corp.*, 4 F.3d at 289–90. In *Raab*, the plaintiffs alleged that the defendant failed to disclose the adverse impact of a contracting slowdown on its earnings and predictions of growth in its annual report, which contained optimistic predictions of future growth such as “the DOE Services Group is posed to carry the growth and success of 1991 well into the future.” *Id.* The Fourth Circuit explained that “‘soft,’ ‘puffing’ statements such as these generally lack materiality because the market price of a share is not inflated by vague statements predicting growth” and that “projections of future performance not worded as guarantees are generally not actionable under the federal securities laws.” *Id.* (internal citations omitted).

As another example, In *IBEW Local Union No. 58 Pension Tr. Fund & Annuity Fund v. Royal Bank of Scot. Grp., PLC*, the plaintiffs alleged that the defendant RBS’s statements in press releases and conference calls regarding its acquisition of another company, including that “[t]he integration of ABN AMRO is off to a promising start,’ ‘[our] positive view . . . has been confirmed,’ [and] ‘we are happy we bought what we thought we bought,’ were misleading

according to plaintiffs, because by December 2007, ABN AMRO was suffering significant losses and the acquisition was ‘an unmitigated disaster for RBS.’” 783 F.3d 383, 392 (2d Cir. 2015). The Second Circuit explained that “statements of corporate optimism may be actionable securities violations if ‘they are worded as guarantees or are supported by specific statements of fact, or if the speaker does not genuinely believe them.’” *Id.* But because the statements were not worded as guarantees and there were no allegations that the defendants did not reasonably believe them, the Second Circuit held that these statements were “inactionable puffery.” *Id.*

Defendants statements of optimism here, including that “the prospects of the combined company are favorable,” that Defendants “are even more convinced in the tremendous opportunity” presented by the merger, and are “excited about the power of the combined companies and the upside growth opportunities” are notably similar to the statements in *Raab* and *Local IBEW*. Nothing in these statements can be taken as a guarantee of success. Nor does plaintiff present factual allegations to suggest that Defendants did not reasonably believe the statements regarding the overall prospects of the merger were favorable when they were made.

Second, and relatedly, these statements of optimism are unactionable statements of opinion. Generally, statements of opinion are not actionable. *Longman v. Food Lion, Inc.*, 197 F.3d at 683. An opinion can be false if (1) the speaker does not actually hold the stated belief; (2) a statement begins with an opinion word like “I believe” but contains an embedded statement of fact that is false; or (3) the statement omits material facts about the speaker’s “inquiry into or knowledge concerning a statement of opinion” and those facts “conflict with what a reasonable investor would take from the statement itself.” *Omnicare, Inc. v. Laborers Dist. Council Const. Indus. Pension Fund*, 575 U.S. 175, 184–85, 189 (2015). Regarding this third category, “whether an omission makes an expression of opinion misleading always depends on context.” *Id.* at 190.

Further, “[a]n opinion statement . . . is not necessarily misleading when an issuer knows, but fails to disclose some fact cutting the other way” as “[r]easonable investors understand that opinions sometimes rest on a weight of competing facts.” *Id.* at 189–90.

As discussed above, Plaintiff does not plead factual allegations to suggest that Defendants did not actually believe any of the statements of optimism. Plaintiff also does not allege that there were embedded statements of fact that were false. Rather, Plaintiff argues that the positive statements about the due diligence gave investors false impressions regarding cybersecurity due diligence and risks. But the Defendants’ positive statements regarding the expected overall success of the merger say nothing about cybersecurity and did not give rise to a duty to provide information about cybersecurity. *See Matrixx Initiatives, Inc. v. Siracusano*, 563 U.S. at 44–45; *Basic Inc. v. Levinson*, 485 U.S. at 239 n.17.

Plaintiff argues that not all the alleged statements of optimism are opinions, citing to the statements in paragraphs 464 and 489 as examples. Pl. Opp. at 33. This argument is unavailing. In the statement alleged in paragraph 464, taken from Marriott’s March 21, 2016 conference call regarding the amended merger agreement with investors, Ms. Oberg discussed updated synergies and earnings per share estimates:

*After we’ve had extensive due diligence and spending a lot of time with the Starwood team and joint integration planning*, we increased our targeted annual G&A cost synergies to \$250 million, up from \$200 million. And excluding any benefit from even more incremental cost savings beyond the \$250 million and additional revenue synergies which we’re confident we will provide, we expect adjusted EPS to be roughly neutral in 2017 and 2018.

¶ 464 (March 21, 2016, Conference Call to Discuss Amended Merger Agreement). In the statement alleged in paragraph 489, taken from Marriott’s second quarter 2016 earnings call, Mr. Sorenson discussed the project timeline for completing the integration:

The Starwood transaction should be completed in the coming weeks bringing these terrific teams together. ***Both the Marriott and Starwood teams have done exhaustive planning to get ready*** and we are excited by our prospects. While we will see a lot of progress in the near-term, we expect that full integration will be a two-year project.

¶ 489 (July 28, 2016, Q2 2016 Earnings Call).

To begin with, Plaintiff only alleges that the portions of these statements regarding Marriott's extensive due diligence and time spent integration planning – indicated by the text bold and italicized – were material misrepresentations. *See* ¶ 202 n.173 (“The statements that are bolded and italicized in this section are statements alleged to be false or misleading.”). For the reasons discussed above in the Section I.a.i, Plaintiff's allegations with respect to those portions of the statement fail. Any additional claim that another part of this statement is false fails because it cannot satisfy the PSLRA's specificity requirement to identify the allegedly false or misleading statement. 15 U.S.C. § 78u-4(b)(1). Even if I considered the other portions of these statements as allegedly false and misleading, contrary to Plaintiff's allegations of what was false or misleading, the remaining portions of these statements are opinion. In the statement alleged in paragraph 464, Ms. Oberg gave projections based on Marriott's beliefs and what they “expect” will happen. Although this expectation was grounded in Marriott's due diligence, that does not turn the statement from an opinion about what Marriott expects to happen to a statement of fact about what will happen. Likewise, Mr. Sorenson's statement alleged in paragraph 489 that Marriott is “excited” about the prospects for the combined companies and that Marriott “expects” that full integration will take two years are statements of opinion, not fact. Therefore, these statements and the other alleged statements of optimism are opinion statements, and Plaintiff fails to allege facts indicating that these opinions were false, misleading, or contained material omissions that were required to be disclosed.

Finally, the statements of optimism fall into the PSLRA's safe harbor for forward looking statements and the "bespeaks caution" doctrine. The PSLRA precludes liability for statements if they are identified as "forward looking statements" and are (1) accompanied by "meaningful cautionary language" or (2) immaterial. 15 U.S.C. § 78u-5(i)(1); *see also In re Constellation Energy Grp., Inc. Sec. Litig.*, 738 F. Supp. 2d 614, 625 (D. Md. 2010). "Similarly, under the judge-made 'bespeaks caution' doctrine, 'cautionary language in an offering document, as part of the total mix' of information, may negate the materiality of an alleged misstatement or omission." *In re Constellation Energy Grp., Inc. Sec. Litig.*, 738 F. Supp. 2d at 625 (citing *Recupito v. Prudential Sec., Inc.*, 112 F. Supp. 2d 449, 455 (D. Md. 2000); *Gasner v. Board of Supervisors*, 103 F.3d 351, 358 (4th Cir.1996)); *see also In re QLT Inc. Sec. Litig.*, 312 F. Supp. 2d 526, 532 (S.D.N.Y. 2004) (the "bespeaks caution" doctrine "operates in a similar fashion [to the PSLRA safe harbor] and protects forward-looking statements accompanied by adequate cautionary language from being actionable."). Of course, vague or boilerplate disclaimers will not suffice as meaningful cautionary language. *In re Constellation Energy Grp., Inc. Sec. Litig.*, 738 F. Supp. 2d at 625. Rather, the cautionary language must contain detailed language tailored to the specific risks the company faces. *Id.*

Here each of the alleged statements of optimism was preceded by a disclaimer regarding forward looking statements. For example, in the December 22, 2015, Form S-4 Registration Statement and its January 27, 2016 and February 16, 2016 amendments, which accompanied the statements alleged to be false or misleading in paragraph 449, is the following statement:

#### SPECIAL NOTE ABOUT FORWARD-LOOKING STATEMENTS

This joint proxy statement/prospectus, including information included or incorporated by reference, contains forward-looking statements within the meaning of the Private Securities Litigation Reform Act of 1995. You can typically identify forward-looking statements by the use of forward-looking words such as "expect,"

“anticipate,” “target,” “goal,” “project,” “intend,” “plan,” “believe,” “budget,” “should,” “continue,” “could,” “forecast,” “may,” “might,” “potential,” “strategy,” “will,” “would,” “seek,” “estimate,” or variations of such words and similar expressions, although the absence of any such words or expressions does not mean that a particular statement is not a forward-looking statement. It is important to note that Starwood’s and Marriott’s goals and expectations are not predictions of actual performance. Any statements about the benefits of the Combination Transactions, or Starwood’s or Marriott’s future financial condition, results of operations and business are also forward-looking statements. Without limiting the generality of the preceding sentence, certain statements contained in the sections entitled “The Combination Transactions—Background of the Combination Transactions,” “The Combination Transactions—Starwood’s Reasons for the Combination Transactions; Recommendation of Starwood’s Board,” “The Combination Transactions—Marriott’s Reasons for the Combination Transactions; Recommendation of Marriott’s Board,” “The Combination Transactions—Opinions of Starwood’s Financial Advisors” and “The Combination Transactions—Opinion of Marriott’s Financial Advisor” may also constitute forward-looking statements.

These forward-looking statements represent Starwood’s and Marriott’s intentions, plans, expectations, assumptions and beliefs about future events, including the completion of the Combination Transactions, and are subject to risks, uncertainties and other factors. Many of these factors are outside the control of Starwood and Marriott and could cause actual results to differ materially from the results expressed or implied by these forward-looking statements. In addition to the risk factors described in the section entitled “Risk Factors” beginning on page 31 of this joint proxy statement/prospectus, these factors include:

- those identified and disclosed in public filings with the SEC made by Starwood and Marriott;
- failing to obtain Starwood and Marriott stockholder approval of the Combination Transactions;
- satisfying the conditions to the closing of the Combination Transactions;
- the length of time necessary to complete the Combination Transactions;
- Starwood’s ability to consummate the spin-off of Vistana and Vistana’s subsequent merger with a subsidiary of ILG or an alternative disposition of Vistana or to realize the anticipated benefits of the Vistana-ILG transactions or an alternative disposition of Vistana;
- successfully integrating the Starwood and Marriott businesses, and avoiding problems which may result in Marriott not operating as effectively and efficiently as expected following the completion of the Combination Transactions;
- the possibility that the expected benefits of the Combination Transactions will not be realized within the expected time frame or at all;
- prevailing economic, market and business conditions;

- the cost and availability of capital and any restrictions imposed by lenders or creditors;
- changes in the industry in which Starwood and Marriott operate;
- conditions beyond Starwood's or Marriott's control, such as disaster, acts of war or terrorism;
- the weather and other natural phenomena, including the economic, operational and other effects of severe weather or climate events, such as tornadoes, hurricanes, ice, sleet, or snowstorms;
- the failure to renew, or the revocation of, any license or other required permits;
- unexpected charges or unexpected liabilities arising from a change in accounting policies, or the effects of acquisition accounting varying from the companies' expectations;
- the risk that the credit ratings of Marriott or its subsidiaries following the completion of the Combination Transactions may be different from what the companies expect, which may increase borrowing costs and/or make it more difficult for Marriott to pay or refinance the debts of Marriott and its subsidiaries and require Marriott to borrow or divert cash flow from operations in order to service debt payments;
- the effects on the companies' businesses resulting from uncertainty surrounding the Combination Transactions, including uncertainty for customers, employees, hotel owners, hotel franchisees, labor unions or suppliers, or the diversion of management's time and attention;
- adverse outcomes of pending or threatened litigation or governmental investigations;
- the effects on the companies of future regulatory or legislative actions, including changes in laws and regulations to which Starwood, Marriott or their subsidiaries are subject;
- the conduct of and changing circumstances related to third-party relationships on which Starwood and Marriott rely, including the level of creditworthiness of counterparties;
- the volatility and unpredictability of stock market and credit market conditions;
- fluctuations in interest rates;
- variations between the stated assumptions on which forward-looking statements are based and Starwood's and Marriott's actual experience; and
- other economic, business, and/or competitive factors.

For any forward-looking statements made in this joint proxy statement/prospectus or in any documents incorporated by reference, Starwood and Marriott claim the protection of the safe harbor for forward-looking statements contained in the Private Securities Litigation Reform Act of 1995. All subsequent written and oral forward-looking statements concerning the Combination Transactions or other matters addressed in this joint proxy statement/prospectus and attributable to Starwood, Marriott or any person acting on their behalf are expressly

qualified in their entirety by the cautionary statements contained or referred to in this joint proxy statement/prospectus.

You are cautioned not to place undue reliance on forward-looking statements, which speak only as of the date of this joint proxy statement/prospectus and should be read in conjunction with the risk factors and other disclosures contained or incorporated by reference into this joint proxy statement/prospectus. The areas of risk and uncertainty described above, which are not exhaustive, should be considered in connection with any written or oral forward-looking statements that may be made in this joint proxy statement/prospectus or on, before or after the date of this joint proxy statement/prospectus by Starwood or Marriott or anyone acting for any or both of them. Except as required by applicable law or regulation, neither Starwood nor Marriott undertake any obligation to release publicly or otherwise make any revisions to any forward-looking statements, to report events or circumstances after the date of this joint proxy statement/prospectus or to report the occurrence of unanticipated events.

Additional factors that could cause actual results to differ materially from those expressed in the forward-looking statements are discussed in reports filed with the SEC by Starwood and Marriott. For a list of the documents incorporated by reference, see the section entitled “Where You Can Find More Information” beginning on page [190].

Def. Ex. A, ECF No. 647-2 at 3–4; 11–12, 19–20.<sup>4</sup> The same filings included additional cautionary language regarding the merger with Starwood:

#### Uncertainties, Risks and Potentially Negative Considerations

In the course of its deliberations, Marriott’s Board also considered a variety of uncertainties, risks and other potentially negative considerations relevant to the transaction, including the following:

- The restrictions on the conduct of Marriott’s business during the period between the execution of the merger agreement and the completion of the Combination Transactions;

---

<sup>4</sup> The Court may take judicial notice of the SEC filings included in Defendant’s Exhibit A, because they are public documents referenced in and integral to the Complaint. *See Yates v. Mun. Mortg. & Equity, LLC*, 744 F.3d at 881 (4th Cir. 2014) (“And as did the district court, we take judicial notice of the content of relevant SEC filings and other publicly available documents included in the record.”); *In re Royal Ahold N.V. Sec. & ERISA Litig.*, 351 F. Supp. 2d 334, 349 (D. Md. 2004) (“In considering a motion to dismiss a securities fraud complaint, the Court is entitled to rely on public documents quoted by, relied upon, incorporated by reference or otherwise integral to the complaint, and such reliance does not convert such a motion into one for summary judgment.” (internal quotation marks omitted)).

- The costs associated with completing the Combination Transactions and realizing the benefits Marriott expects to obtain in connection with the Combination Transactions, including management's time and energy and potential opportunity cost;
- The challenges in absorbing the effect of any failure to complete the Combination Transactions, including potential termination fees and stockholder and market reactions;
- The potential earnings dilution to Marriott stockholders following the closing of the Combination Transactions;
- The challenges inherent in combining two businesses of the size and complexity of Starwood and Marriott, including the possible diversion of management and employee attention for an extended period of time;
- The potential for diversion of management and employee attention during the period before completion of the Combination Transactions, and the potential negative effects on Marriott's and the combined company's business;
- The risk that certain provisions in certain of Starwood's and Marriott's contracts may constrain or delay the timing for realizing, operational and development plans, synergies, cost savings and other anticipated benefits expected to result from a combination of Starwood and Marriott;
- The difficulties of combining the businesses and workforces of Starwood and Marriott based on, among other things, differences in the cultures of the two companies, union and collective bargaining agreements, and other factors;
- The risk that regulatory agencies may object to and challenge the Combination Transactions or may impose terms and conditions in order to resolve those objections that adversely affect the financial results of the combined company; see the section entitled "—Regulatory Clearances Required for the Combination Transactions" beginning on page 117;
- The risk that hotel owners and hotel franchisees with whom Starwood and Marriott have contractual relationships may not view the Combination Transactions favorably and those relationships may be negatively impacted as a result;
- Starwood's right, subject to certain conditions, to respond to and negotiate on certain alternative takeover proposals made before the time Starwood stockholders approve the Starwood combination transactions proposal and the right of Starwood's Board to withdraw or modify in a manner adverse

to Marriott its recommendation to Starwood stockholders with respect to the Starwood combination transactions proposal, subject to Starwood paying Marriott a termination fee of \$400 million if Starwood elects to terminate the merger agreement as a result;

- The risk that Starwood stockholders or Marriott stockholders may object to and challenge the Combination Transactions and take actions that may prevent or delay the consummation of the Combination Transactions, including voting down the proposals at the Starwood or Marriott special meetings; and
- The potential that the fixed exchange ratio under the merger agreement could result in Marriott delivering greater value to Starwood stockholders than had been anticipated by Marriott should the value of the shares of Marriott common stock increase from the date of the execution of the merger agreement.

Further, Marriott's Board considered that some members of Marriott's Board and certain Marriott executive officers may have interests in the proposed Combination Transactions as individuals that are in addition to, and that may be different from, the interest of Marriott stockholders generally, as described under "—Interests of Marriott Directors and Executive Officers in the Combination Transactions" beginning on page 117.

After considering these potentially positive and potentially negative reasons, Marriott's Board unanimously concluded, in its business judgment, that the potentially positive reasons relating to the merger agreement and the transactions contemplated thereby (including the issuance of shares of Marriott common stock to Starwood stockholders) outweighed the potentially negative reasons.

The foregoing discussion of the information and reasons considered by Marriott's Board is not exhaustive but is intended to reflect the material reasons considered by Marriott's Board in its evaluation of the Combination Transactions. In view of the complexity, and the large number, of the reasons considered, Marriott's Board, both individually and collectively, did not find it practicable to, and did not attempt to, quantify or assign any relative or specific weight to the various reasons. Rather, Marriott's Board based its recommendation on the totality of the information presented to and considered by it. In addition, individual members of Marriott's Board may have given different weight to different reasons.

The foregoing discussion of the information and reasons considered by Marriott's Board is forward-looking in nature. This information should be read in light of the reasons described under "Special Note About Forward-Looking Statements" beginning on page 42.

*Id.* at 7–8, 15–16, 23–24. Marriott’s other SEC filings in question contain similar cautionary language. *See id.* at 28–29, 32–33, 40–49, 56, 59, 62–73, 80–90, 93–103, 106–13, 116–26, 129–39, 142–52, 155–64, 167–77, 180–90, 193–03.

Marriott also included cautionary language before its investor conference calls. For example, at the beginning of the March 21, 2016 conference call with investors regarding the amended merger agreement, prior to the statements alleged in paragraph 465, Ms. Oberg stated:

As always, before we get into the discussion today, let me first remind everyone that many of our comments are not historical facts and are considered forward-looking statements under federal securities law. These statements are subject to numerous risks and uncertainties, as described in our SEC filings, which could cause future results to differ materially from those expressed in or implied by our comments. Forward-looking statements in the press release that we issued this morning, along with our comments today, are effective only today, March 21, 2016, and will not be updated as actual events unfold.

*Id.* at 52. Marriott’s other conference calls with investors in question contain similar cautionary language. *See id.* at 35–37, 76.

These cautionary statements are detailed and highly specific to Marriott and the Starwood transaction, and therefore qualify as meaningful cautionary statements for the purposes of the PSLRA and the bespeaks caution doctrine. *Cf. Gasner v. Bd. of Sup’rs of the Cty. of Dinwiddie, Va.*, 103 F.3d 351, 359 (4th Cir. 1996) (finding cautionary language not boilerplate where it “describes in specific detail the risks which a purchaser would assume” and “no guarantee” risk would not materialize).

Plaintiff cites *Lefkoe v. Jos. A. Bank Clothiers* for the proposition that “the adequacy of cautionary language is a question of fact, and, typically, is not a question to be resolved on a motion to dismiss.” No. CIV WMN-06-1892, 2007 WL 6890353, at \*5–7 (D. Md. Sept. 10, 2007) (citing *Blatt v. Corn Products Intern., Inc.*, No. 05-C-3033, 2006 WL 1697013, at \*5 (N.D. Ill. June 14, 2006)). That may be so as a general matter. But I may properly consider the cautionary statements

on a motion to dismiss in appropriate circumstances. *See, e.g., Hillson Partners Ltd. P'ship v. Adage, Inc.*, 42 F.3d 204, 218–19 (4th Cir. 1994) (affirming dismissal of securities claim under § 10(b) and Rule 10b-5 on a motion to dismiss including because of cautionary language); *In re USEC Sec. Litig.*, 190 F. Supp. 2d 808, 825 (D. Md. 2002), (dismissing securities claim on a motion to dismiss including because of cautionary language), *aff'd and remanded sub nom. Cohen v. USEC, Inc.*, 70 F. App'x 679 (4th Cir. 2003). Here, besides disparaging the cautionary statements as “boilerplate,” Plaintiff does not provide any allegations or arguments as to why Plaintiff’s cautionary language is inadequate. Plaintiff’s conclusory statement that these detailed cautionary statements are boilerplate is insufficient to create a question of fact that would preclude their consideration here.

Plaintiff also argues that some of the statements are not forward looking at all and cites the statement alleged in paragraph 464 as an example.<sup>5</sup> Pl. Opp. at 33. Once again, the statement alleged in paragraph 464 is taken from Marriott’s March 21, 2016 conference call with investors. There Ms. Oberg stated:

*After we've had extensive due diligence and spending a lot of time with the Starwood team and joint integration planning*, we increased our targeted annual G&A cost synergies to \$250 million, up from \$200 million. And excluding any benefit from even more incremental cost savings beyond the \$250 million and additional revenue synergies which we're confident we will provide, we expect adjusted EPS to be roughly neutral in 2017 and 2018.

¶ 464 (March 21, 2016, Conference Call to Discuss Amended Merger Agreement). Like the statements discussed above, the only portion of this statement that is alleged to be a material misrepresentation relates to Marriott’s due diligence and integration planning. That allegation fails

---

<sup>5</sup> Plaintiff also argues that the statement alleged in paragraph 466 is not a forward-looking statement. I agree. This statement is not included in the discussion of this section. It is discussed as one of the statements regarding due diligence and integration in Section I.a.i.

for the reasons discussed in Section I.a.i above. Additional allegations that other portions of this statement were false or misleading fails for lack of specificity. If I were to consider the remaining portion of the statement in paragraph 464 as false or misleading, that portion of the statement is forward-looking as it pertains to Marriott's "targeted" synergies and "expected" earnings per share.

Finally, Plaintiff argues that the PSLRA's safe harbor does not apply to material omissions. Pl. Opp. at 33–34. In support of this proposition, Plaintiffs cite *Wilson v. LSB Indus., Inc.*, 2017 WL 7052046, at \*3 (S.D.N.Y. Mar. 2, 2017). *Wilson* and the line of cases it derives from within the Second Circuit hold that the safe harbor for forward-looking statements does not protect material omissions insofar as material omissions must be omissions of historical fact. *See, e.g., In re Complete Mgmt. Inc. Sec. Litig.*, 153 F. Supp. 2d 314, 340 (S.D.N.Y. 2001) ("The 'bespeaks causation' doctrine, and the related statutory 'safe harbor' provision of the PSLRA . . . apply to forward-looking statements *only*, and not to material omissions or misstatements of historical fact."); *In re Oxford Health Plans, Inc.*, 187 F.R.D. 133, 141 (S.D.N.Y. 1999) ("Defendants do not claim that all of the alleged misrepresentations are forward-looking or that omissions can even be forward-looking. . . . The safe harbor and bespeaks caution doctrines do not apply to these omissions."). However, because Plaintiff fails to allege that the forward-looking statements are false or misleading, it also fails to allege that Marriott made material omissions regarding data security. *Matrixx Initiatives, Inc. v. Siracusano*, 563 U.S. at 44 ("Disclosure is required under [Section 10(b) and Rule 10b-5] only when necessary 'to make . . . statements made, in the light of the circumstances under which they were made, not misleading.'") (quoting 17 CFR § 240.10b-5(b)); *see also Basic Inc. v. Levinson*, 485 U.S. 224, 239 n.17 ("Silence, absent a duty to disclose, is not misleading under Rule 10b-5."). Therefore, because Plaintiff fails to adequately allege that the statements of optimism contained material omissions, its reliance on these cases fails.

### iii. Risk Factor Disclosures

Plaintiff alleges that Marriott's risk factor disclosures in its SEC statements were false and misleading. *See ¶¶ 458, 460, 483, 485, 492, 494, 503, 505, 513, 515, 519, 522, 528, 530, 537, 539, 551, 553, 557, 560, 564, 567, 585, 587.* Marriott is required to include in its SEC filings a section on risk factors that has "a discussion of the material factors that make an investment in the registrant or offering speculative or risky." 17 C.F.R. § 229.105 (Reg. S-K, Item 105).

"Though ubiquitous in securities filings . . . cautionary statements of potential risk have only rarely been found to be actionable by themselves." *In re FBR Inc. Sec. Litig.*, 544 F. Supp. 2d 346, 360–61 (S.D.N.Y. 2008) (*citing Libon v. Infineon Techs., AG*, No. 04 Civ. 929, 2006 U.S. Dist. LEXIS 76430, at \*26 (E.D.Va. Aug. 7, 2006) (Lauck, M.J.)). In *In re ChannelAdvisor Corp. Sec. Litig.*, a court within this circuit reviewed caselaw on risk disclosures:

Only one circuit court appears to have addressed the materiality of risk factor disclosures. In *Bondali v. Yum! Brands, Inc.*, the Sixth Circuit held cautionary statements inactionable "to the extent plaintiffs contend defendants should have disclosed risk factors 'are' affecting financial results rather than 'may' affect financial results." 620 Fed. Appx. 483, 491 (6th Cir. 2015) (quoting *In re FBR Inc. Sec. Litig.*, 544 F. Supp. 2d 346, 362 (S.D.N.Y. 2008)). According to that court, this is because of the "inherently prospective" nature of such disclosures, which "are not meant to educate investors on what harms are currently affecting the company." *Id.* Thus, the Sixth Circuit concluded that "a reasonable investor would be unlikely to infer anything regarding the current state of a corporation's compliance, safety, or other operations from a statement intended to educate the investor on *future* harms." *Id.*

No. 5:15-CV-00307-F, 2016 WL 1381772, at \*5 (E.D.N.C. Apr. 6, 2016). In that case, the Defendant included in its risk factor disclosures that it could face a decline in revenue if more customers demanded contracts with fixed pricing. *Id.* The plaintiffs alleged that this disclosure was materially misleading because the defendants knew at the time of the disclosure that a pronounced shift of its customer base to contracts with fixed pricing was occurring. *Id.* The court dismissed the plaintiffs' claims on the basis that a reasonable investor likely would not, from the

cautionary language, infer anything about the defendants' current contracts. *Id.* at \*6. The Fourth Circuit affirmed. *Dice v. Channeladvisor Corp.*, 671 F. App'x 111 (4th Cir. 2016).

Other courts have held that risk factor disclosures could be materially misleading if the defendant knew or was recklessly ignorant that the risk was already occurring. *See In re Van der Moolen Holding N.V. Sec. Litig.*, 405 F. Supp. 2d 388, 400 (S.D.N.Y. 2005) ("[T]o warn that the untoward may occur when the event is contingent is prudent; to caution that it is only possible for the unfavorable events to happen when they have already occurred is deceit."") (quoting *Voit v. Wonderware Corp.*, 977 F. Supp. 363, 371 (E.D. Pa. 1997), *abrogated on other grounds by In re Advanta Corp. Sec. Litig.*, 180 F.3d 525 (3d Cir. 1999)). In *Van der Moolen Holding N.V. Sec. Litig.*, the court found that the plaintiffs had plausibly alleged that the defendants' risk factor disclosure regarding legal and regulatory risks were material misrepresentations because the defendants knew or were recklessly ignorant in not knowing that its employees at the time were violating New York Stock Exchange rules. *Id.*; *see also Paskowitz v. Arnall*, 2019 WL 3841999, at \*8 (W.D.N.C. Aug. 15, 2019) (collecting cases for proposition that a risk disclosure that discusses a risk that has already come to fruition as "potential" could be false or misleading).

Here Marriott included risk factor disclosures in its SEC filings and statements to investors regarding the Starwood merger. For example:

The combined company may not be able to integrate successfully and many of the anticipated benefits of combining Starwood and Marriott may not be realized. ***We entered into the Merger Agreement with the expectation that the Starwood Combination will result in various benefits, including, among other things, operating efficiencies. Achieving those anticipated benefits is subject to a number of uncertainties, including whether we can integrate the business of Starwood in an efficient and effective manner.***

***The integration process could also take longer than we anticipate and could result in the loss of valuable employees, the disruption of each company's ongoing businesses, processes and systems or inconsistencies in standards, controls, procedures, practices, policies and compensation arrangements, any of***

*which could adversely affect the combined company's ability to achieve the benefits we anticipate.* The combined company's resulting portfolio of approximately 30 brands could be challenging for us to maintain and grow, and *the harmonization of our different reservations and other systems and business practices could be more difficult, disruptive, and time consuming than we anticipate.* *The combined company's results of operations could also be adversely affected by any issues attributable to either company's operations that arise or are based on events or actions that occur before the Starwood Combination closes.* *The combined company may also have difficulty addressing possible differences in corporate cultures and management philosophies.* *The integration process is subject to a number of uncertainties, and we cannot assure you that the benefits we anticipate will be realized at all or as quickly as we expect.* *If we don't achieve those benefits, our costs could increase, our expected net income could decrease, and the combined company's future business, financial condition, operating results and prospects could suffer.*

¶ 458 (February 18, 2016, 2015 Form 10-K); ¶ 483 (April 28, 2016, Q1 2016 Form 10-Q); ¶ 492 (July 28, 2016, Q2 2016 Form 10-Q).

*A failure to keep pace with developments in technology could impair our operations or competitive position. The lodging industry continues to demand the use of sophisticated technology and systems, including those used for our reservation, revenue management, and property management systems, our Marriott Rewards and The Ritz-Carlton Rewards programs, and technologies we make available to our guests. These technologies and systems must be refined, updated, and/or replaced with more advanced systems on a regular basis, and if we cannot do so as quickly as our competitors or within budgeted costs and time frames, our business could suffer. We also may not achieve the benefits that we anticipate from any new technology or system, and a failure to do so could result in higher than anticipated costs or could impair our operating results.*

\*\*\*

*We are exposed to risks and costs associated with protecting the integrity and security of internal and customer data. Our businesses process, use, and transmit large volumes of internal employee and customer data, including credit card numbers and other personal information in various information systems that we maintain and in those maintained by third parties, including our owners, franchisees and licensees, as well as our service providers, in areas such as human resources outsourcing, website hosting, and various forms of electronic communications. The integrity and protection of that customer, employee, and company data is critical to our business. If that data is inaccurate or incomplete, we could make faulty decisions.*

*Our customers and employees also have a high expectation that we, as well as our owners, franchisees, licensees, and service providers, will adequately protect their personal information. The information, security, and privacy requirements imposed by governmental regulation and the requirements of the payment card industry are also increasingly demanding, in both the United States and other jurisdictions where we operate. Our systems and the systems maintained or used by our owners, franchisees, licensees, and service providers may not be able to satisfy these changing requirements and employee and customer expectations, or may require significant additional investments or time in order to do so.*

\*\*\*

*Cyber-attacks could have a disruptive effect on our business. Efforts to hack or breach security measures, failures of systems or software to operate as designed or intended, viruses, operator error, or inadvertent releases of data may materially impact our, including our owners', franchisees', licensees', or service providers', information systems and records. Our reliance on computer, Internet-based and mobile systems and communications and the frequency and sophistication of efforts by hackers to gain unauthorized access to such systems have increased significantly in recent years. A significant theft, loss, or fraudulent use of customer, employee, or company data could adversely impact our reputation and could result in remedial and other expenses, fines, or litigation. Breaches in the security of our information systems or those of our owners, franchisees, licensees, or service providers or other disruptions in data services could lead to an interruption in the operation of our systems, resulting in operational inefficiencies and a loss of profits. In addition, although we carry cyber/privacy liability insurance that is designed to protect us against certain losses related to cyber risks, such insurance coverage may be insufficient to cover all losses or all types of claims that may arise in connection with cyber-attacks, security breaches, and other related breaches.*

\*\*\*

*Any disruption in the functioning of our reservation system, such as in connection with the Starwood Combination, could adversely affect our performance and results. We manage a global reservation system that communicates reservations to our branded hotels that individuals make directly with us online, through our mobile app, or through our telephone call centers, or through intermediaries like travel agents, Internet travel web sites and other distribution channels. The cost, speed, accuracy and efficiency of our reservation system are critical aspects of our business and are important considerations for hotel owners when choosing our brands. Our business may suffer if we fail to maintain, upgrade, or prevent disruption to our reservation system. In addition, the risk of disruption in the functioning of our global reservation system could increase in connection with the system integration that we anticipate undertaking following consummation of the Starwood Combination. Disruptions in or*

*changes to our reservation system could result in a disruption to our business and the loss of important data.*

¶ 460 (February 18, 2016, 2015 Form 10-K); ¶ 485 (February 18, 2016, 2015 Form 10-K); ¶ 494 (July 28, 2016, Q2 2016 Form 10-Q); ¶ 505 (November 9, 2016, Q3 2016 Form 10-Q); ¶ 515 (February 21, 2017, 2016 Form 10-K); ¶ 522 (May 9, 2017, Q1 2017 Form 10-Q); ¶ 530 (August 8, 2017, Q2 2017 Form 10-Q); ¶ 539 (November 8, 2017, Q3 2017 Form 10-Q); ¶ 553 (February 14, 2018, 2017 Form 10-K); ¶ 560 (May 10, 2018, Q1 2018 Form 10-Q); ¶ 567 (August 7, 2018, Q2 2018 Form 10-Q).

We may not be able to integrate Starwood successfully and many of the anticipated benefits of combining Starwood and Marriott may not be realized. *We entered into the Merger Agreement with the expectation that the Starwood Combination will result in various benefits, including, among other things, operating efficiencies. Achieving those anticipated benefits is subject to a number of uncertainties, including whether we can integrate the business of Starwood in an efficient and effective manner.*

*The integration process could also take longer than we anticipate and could result in the loss of valuable employees, the disruption of each company's ongoing businesses, processes and systems or inconsistencies in standards, controls, procedures, practices, policies and compensation arrangements, any of which could adversely affect the combined company's ability to achieve the benefits we anticipate. Our resulting portfolio of approximately 30 brands may be challenging for us to maintain and grow, and the harmonization of our different reservations and other systems and business practices could be more difficult, disruptive, and time consuming than we anticipate. We may also have difficulty addressing possible differences in corporate cultures and management philosophies.* We may incur unanticipated costs in the integration of the businesses of Starwood. Although we expect that the elimination of certain duplicative costs, as well as the realization of other efficiencies related to the integration of the two businesses, will over time offset the substantial incremental transaction and merger-related costs and charges we incurred in connection with the Starwood Combination, we may not achieve this net benefit in the near term, or at all.

*The integration process is subject to a number of uncertainties, and we cannot assure you that the benefits we anticipate will be realized at all or as quickly as we expect. If we don't achieve those benefits, our costs could increase, our expected net income could decrease, and the combined company's future business, financial condition, operating results, and prospects could suffer.*

Our future results will suffer if we do not effectively manage our expanded operations. *With completion of the Starwood Combination, the size of our business has increased significantly. Our future success depends, in part, upon our ability to manage this expanded business, which poses substantial challenges for management, including challenges related to the management and monitoring of new operations and associated increased costs and complexity. We cannot assure you that we will be successful or that we will realize the expected operating efficiencies, cost savings, and other benefits from the combination that we currently anticipate.*

¶ 503 (November 9, 2016, Q3 2016 Form 10-Q); ¶ 513 (February 21, 2017, 2016 Form 10-K); ¶ 519 (May 9, 2017, Q1 2017 Form 10-Q); ¶ 528 (August 8, 2017, Q2 2017 Form 10-Q).

Some of the anticipated benefits of combining Starwood and Marriott may still not be realized. *We decided to acquire Starwood with the expectation that the Starwood Combination will result in various benefits, including, among other things, operating efficiencies. Although we have already achieved some of those anticipated benefits, others remain subject to a number of uncertainties, including whether we can continue to integrate the business of Starwood in an efficient and effective manner and whether, and on what terms, we can reach agreement with the companies that issue our branded credit cards and the timeshare companies with whom we do business to allow us to move to a single unified reservation system and loyalty platform.*

*The integration process could take longer than we anticipate and involve unanticipated costs. Disruptions of each legacy company's ongoing businesses, processes, and systems could adversely affect the combined company. We also may still encounter difficulties harmonizing our different reservations and other systems and business practices as the integration process continues.* As a result of these or other factors, we cannot assure you when or that we will be able to fully realize additional benefits from the Starwood Combination in the form of eliminating duplicative costs, or achieving other operating efficiencies, cost savings, or benefits.

¶ 537 (November 8, 2017, Q3 2017 Form 10-Q); ¶ 551 (February 14, 2018, 2017 Form 10-K); ¶ 557 (May 10, 2018, Q1 2018 Form 10-Q); ¶ 564 (August 7, 2018, Q2 2018 Form 10-Q); ¶ 585 (November 6, 2018, Q3 2018 Form 10-Q).

Importantly, after Marriott learned of the data breach, it updated its risk factor disclosures regarding cyber-security incidents, including the statement, *“Like most large multinational corporations, we 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.” ¶ 587 (November 6, 2018, Q3 2018 Form 10-Q).*

Plaintiff alleges that each of Marriott’s risk factor disclosures in its SEC filings was false and misleading because Marriott “failed to disclose critical facts relevant to these risks that existed at the time, including the vulnerability of the customer data and that the Data Breach was currently ongoing” and the disclosures gave investors “a false impression that Marriott was operating the newly-acquired Starwood systems in accordance with relevant requirements, standards, and best practices” and “a false impression that Marriott had made adequate preparations and dedicated adequate resources to cybersecurity.” *See, e.g., ¶¶ 523, 521.*

To begin with, analysis of Plaintiff’s arguments that Marriott’s risk disclosures were false or misleading must be informed by the facts that Plaintiff has pleaded. Significantly, Plaintiff alleges that Marriott discovered the data breach in September 2018. ¶ 31. Therefore, its risk factor disclosures before then were not false and misleading for not disclosing the Starwood data breach. *Cf. In re Equifax Inc. Sec. Litig.*, 357 F. Supp. 3d 1189, 1225 (N.D. Ga. 2019) (“[T]he Defendants were under no duty to disclose the existence of the Data Breach before they knew it had occurred.”). And Marriott’s risk factor disclosures after the breach was discovered state that “we have experienced cyber-attacks.” ¶ 587. Thus, Plaintiff’s allegation that the risk factor disclosures were false or misleading for failing to disclose that the data breach was ongoing fails.

Plaintiff argues that Marriott’s risk factor disclosure on February 21, 2017 and thereafter that its systems may not be able to keep pace with payment card industry standards were false and misleading because by February 10, 2017 the Board allegedly knew that Starwood was not compliant with the Payment Card Industry Data Security Standards (“PCI DSS”), which Marriott

agreed to abide by as a merchant and processor of credit cards. *See* Pl. Opp. at 31. As included above, the portions of the risk factor disclosures in question state:

***The information, security, and privacy requirements imposed by governmental regulation and the requirements of the payment card industry are also increasingly demanding, in both the United States and other jurisdictions where we operate. Our systems and the systems maintained or used by our owners, franchisees, licensees, and service providers may not be able to satisfy these changing requirements and employee and customer expectations, or may require significant additional investments or time in order to do so.***

¶ 515 (February 21, 2017, 2016 Form 10-K); ¶ 522 (May 9, 2017, Q1 2017 Form 10-Q); ¶ 530 (August 8, 2017, Q2 2017 Form 10-Q); ¶ 539 (November 8, 2017, Q3 2017 Form 10-Q); ¶ 553 (February 14, 2018, 2017 Form 10-K); ¶ 560 (May 10, 2018, Q1 2018 Form 10-Q); ¶ 567 (August 7, 2018, Q2 2018 Form 10-Q).

Plaintiff's allegations regarding PCI DSS compliance are based on those included in a complaint filed in the Chancery Court of Delaware and documents cited in the Chancery Court complaint. ¶ 314. Specifically, Plaintiff cites to a cybersecurity presentation given to the Board that stated Starwood's “[b]rand standards did not mandate PCI compliance, tokenization, or point-to-point encryption.” The Chancery Court complaint also alleges that the same presentation stated that a “key recommendation” to the Board was to “[u]pdate Starwood brand standards to mandate PCI and set cybersecurity expectations” and as “intended actions,” Marriott would “[p]artner with Owner & Franchise Services to communicate and drive adoption of Marriott security standards for Starwood hotels” and “[e]ngage Protiviti to perform an assessment of PCI controls across 40 additional Starwood hotels.” *See* ECF No. 690-1, Def. Ex. C, ¶ 125 (excerpt from Chancery Court complaint).<sup>6</sup> Plaintiff alleges that Marriott's Board received a further update on February 9, 2018

---

<sup>6</sup> The Court may properly consider this excerpt from the Chancery Court complaint included in Defendants' Exhibit C because it is a public document incorporated and referenced in the Complaint, see note 3, *supra*, and because the Court may “take judicial notice of docket entries,

that Marriott had implemented patches to fix Starwood issues and the “[m]igration from Starwood’s systems to Marriott established technology standards for PCs, Laptops and other end user devices” would not be completed until September 2019. ¶ 314.

Thus, the allegations assert that the Board was aware that Starwood did not mandate PCI DSS compliance, that its intended action was to make Starwood compliant with Marriott’s brand standards including PCI DSS compliance, and that it was taking several years to do so. But this is precisely the risk that Marriott warned about in its risk factor disclosures. Marriott stated that it “may not be able to satisfy” the “information, security, and privacy requirements . . . of the payment card industry” or that it “may require significant additional investments or time in order to do so.” *See, e.g.*, ¶ 515. Plaintiff fails to allege how this was not a truthful disclosure or how a reasonable investor could be misled into believing that this statement meant the opposite.

Plaintiff’s allegations that Marriott’s risk factor disclosures were false or misleading because they gave investors the false impression that Marriott was operating Starwood in accordance with a set of best practices and Marriott did not disclose critical facts relevant to the vulnerability of customer data also fail. To the extent Plaintiff alleges that Marriott’s risk factor disclosures were misleading about its *current* state of cybersecurity, those allegations fail because the risk factor disclosures are not intended to educate investors about harms currently affecting the company. *See In re ChannelAdvisor Corp. Sec. Litig.*, No. 5:15-CV-00307-F, 2016 WL 1381772, at \*5 (“[A] reasonable investor would be unlikely to infer anything regarding the current state of a corporation’s compliance, safety, or other operations from a statement intended to educate the

---

pleadings and papers in other cases.” *Brown v. Ocwen Loan Servicing, LLC*, 2015 WL 5008763, at \*1 n.3 (D. Md. Aug. 20, 2015), *aff’d*, 639 F. App’x 200 (4th Cir. 2016).

investor on *future* harms.”) (quoting *Bondali v. Yum! Brands, Inc.*, 620 Fed. App’x 483, 491 (6th Cir. 2015)).

To the extent Plaintiff’s allegations relate to a failure to disclose information about future harms, Plaintiff fails to allege how a reasonable investor could be misled into thinking that Marriott’s detailed risk factor disclosures, including that “[c]yber-attacks could have a disruptive effect on our business,” would suggest the opposite. Likewise, Plaintiff fails to allege how a reasonable investor could be misled into thinking that Marriott’s disclosures warning that it may not be able to meet regulatory and governmental requirements meant that it was employing a specific set of best practices identified by Plaintiff. In sum, Plaintiff’s allegations fail to plausibly demonstrate that the risk factor disclosures could be false or misleading to a reasonable investor. Marriott was not required to disclose more. *See In re ChannelAdvisor Corp. Sec. Litig.*, No. 5:15-CV-00307-F, 2016 WL 1381772, at \*6 (“Rule 10b-5 does not contain a ‘freestanding completeness requirement’ because ‘[n]o matter how detailed and accurate disclosure statements are, there are likely to be additional details that could have been disclosed but were not.’”) (quoting *In re Intuitive Surgical Sec. Litig.*, 65 F. Supp. 3d 821, 836 (N.D. Cal. Aug. 21, 2014) (quoting *Brody v. Transitional Hosps. Corp.*, 280 F.3d 997, 1006 (9th Cir. 2002))).

Finally, because Plaintiff fails to allege that the risk factor disclosures are false or misleading, it also fails to allege that Marriott made material omissions regarding data security. *Matrixx Initiatives, Inc. v. Siracusano*, 563 U.S. at 44 (“Disclosure is required under [Section 10(b) and Rule 10b-5] only when necessary ‘to make . . . statements made, in the light of the circumstances under which they were made, not misleading.’”) (quoting 17 CFR § 240.10b-5(b)).

#### **iv. Statements Regarding Protecting Customer Data**

Plaintiff alleges that Defendants' statements regarding the importance of protecting customer data were false and misleading. *See ¶¶ 456, 460, 485, 494, 505, 510, 515, 522, 530, 539, 549, 553, 560, 567, 587.* Specifically, Marriott included the following statements in its SEC filings:

Keeping pace with developments in technology is important for our operations and our competitive position. Furthermore, ***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.

¶ 456 (February 18, 2016, 2015 Form 10-K); ¶ 510 (February 21, 2017, 2016 Form 10-K); ¶ 549 (February 14, 2018, 2017 Form 10-K). Marriott also included the following statement in its risk factor disclosures, as quoted above.

***Our customers and employees also have a high expectation that we, as well as our owners, franchisees, licensees, and service providers, will adequately protect their personal information.***

*See, e.g.*, ¶ 460 (February 18, 2016, 2015 Form 10-K). Plaintiff alleges that these statements were false or misleading because at the time they were made, Starwood's IT systems were severely vulnerable and gave investors a false impression that Marriott made adequate preparations and dedicated adequate resources to cybersecurity. *See, e.g.*, ¶¶ 453–54, 457.

Defendants argue that these statements constitute general commitments to safeguard customer data and are unactionable puffery. Several Courts have agreed, and found general commitment statements to safeguard data to be unactionable puffery. For example, in *In re Alphabet, Inc. Sec. Litig.*, a court in the Northern District of California found that “generalized statements regarding the importance of privacy to users and Alphabet's general commitment to transparency and protection of their users' data . . . are too vague and generalized to constitute the bases for misrepresentations; they are merely unactionable puffery.” No. 18-CV-06245-JSW, 2020 WL 2564635, at \*4 (N.D. Cal. Feb. 5, 2020). Similarly, in *In re Constellation Energy Grp., Inc.*

*Sec. Litig.*, a court in this District found that the defendant's statements that it had a strong risk management program, "stating for example that the company's approach to risk management 'is predicated on a strong risk management culture combined with an effective system of internal controls,'" were unactionable puffery. No. CIV. CCB-08-02854, 2012 WL 1067651, at \*11 (D. Md. Mar. 28, 2012). The court explained that the statements "were vague enough that 'a reasonable investor would not depend on [them].'" . . . In other words, '[n]o investor would take such statements seriously in assessing a potential investment, for the simple fact that almost every [similar company] makes these statements.'" *Id.* at \*12 (quoting *ECA & Local 134 IBEW Joint Pension Trust of Chicago v. JP Morgan Chase Co.*, 553 F.3d 187, 206 (2d Cir. 2009)). See also *Lasker v. New York State Elec. & Gas Corp.*, 85 F.3d 55, 59 (2d Cir. 1996) (finding statements regarding "commitment to create earning opportunities" unactionable puffery); *In re Extreme Networks, Inc. Sec. Litig.*, 2018 WL 1411129, at \*23 (N.D. Cal. Mar. 21, 2018) (finding statements about "commitment" to achieve 10% revenue growth and 10% operating margin unactionable puffery); *Rochester Laborers Pension Fund v. Monsanto Co.*, 883 F. Supp. 2d 835, 890 (E.D. Mo. 2012) (finding statement that defendant was "'committed to' reaching the predicted goals" unactionable puffery).

Here the statements that data protection is "critical" to Marriott is general, aspirational language akin to and being "committed" to reaching particular goals. Marriott was in no way certifying that it would not be the victim of a data breach or that it used particular methods to secure data. Cf. *Lasker v. New York State Elec. & Gas Corp.*, 85 F.3d 55, 59 (2d Cir. 1996) (Defendant "was not representing that its actions would in no way impact the company's finances. Nor did it certify that the company would not suffer losses . . . [and] was in no way insuring that dividend rates would remain constant, or that the stock price would not decline.")

Plaintiff cites *Equifax*, in which the court did find statements about Equifax’s commitment to data security actionable. *Equifax*, 357 F. Supp. 3d at 1224–25. There the court reasoned that it could not, as a matter of law, find that such statements were immaterial to reasonable investors. *Id.* The court found it significant that the statements related to a core aspect of Equifax’s business and that they were made repeatedly. *Id.* at 1224. While the court did not list all of the statements it considered within this category, it repeatedly cited Equifax’s statements that it had “strong data security and confidentiality standards” and maintained “a highly sophisticated data information network that includes advanced security, protections and redundancies.” *In re Equifax Inc. Sec. Litig.*, 357 F. Supp. 3d 1189, 1207 (N.D. Ga. 2019). These statements are of a character that could be proven true or false and cross the line from puffery into material statements. *Cf. Dunn v. Borta*, 369 F.3d 421, 431 (4th Cir. 2004) (“[W]hen a proposed seller goes beyond [mere exaggeration of the qualities which an article has], assigns to the article qualities which it does not possess, does not simply magnify in opinion the advantages which it has but invents advantages and falsely asserts their existence, he transcends the limits of ‘puffing’ and engages in false representations and pretenses.”) (quoting *United States v. New S. Farm & Home Co.*, 241 U.S. 64, 71 (1916); *In re Massey Energy Co. Securities Litigation*, 883 F. Supp. 2d 597, 614 (S.D. W. Va. 2012) (finding “the truth or falsity” of defendant’s statements that it was an “industry leader in safety” could be determined and therefore actionable). In contrast, Marriott’s statements that data protection was “critical” are not specific and verifiable and do not assign a quality to Marriott’s cybersecurity that it did not have; indeed, unlike the statements found to be actionable in *Equifax*, Marriott made no characterization at all with respect to the quality of its cybersecurity, only that Marriott considered it important.

Regarding the statement that Marriott's customers and employees have a "high expectation" that Marriot protects their personal information, Plaintiff fails to allege any facts suggesting that Marriott's customers and employees did not have this expectation. Rather, the central premise of the Complaint is that they *did* have an expectation that customers' personal information would be protected. Therefore, Plaintiff fails to allege that this statement was false. Likewise, Plaintiff fails to allege that a reasonable investor could be misled by this statement. It provided no guarantees of cybersecurity or that Marriott would take specific actions regarding cybersecurity. In fact, this statement was made as part of the risk factor disclosures warning that Marriott may not be able to protect customer data from a cyber-attack. Plaintiff provides no allegations how a reasonable investor could reach the opposite conclusion based on this disclosure.

Because Plaintiff fails to allege that the statements regarding protecting customer data are false or misleading, it also fails to allege that these statements contain material omissions. *Matrixx Initiatives, Inc. v. Siracusano*, 563 U.S. at 44 ("Disclosure is required under [Section 10(b) and Rule 10b-5] only when necessary 'to make . . . statements made, in the light of the circumstances under which they were made, not misleading.'") (quoting 17 CFR § 240.10b-5(b)).

#### **v. Privacy Statements**

Plaintiff alleges that Marriott's global privacy statements were false and misleading. *See* ¶¶ 498, 534, 571. These privacy statements were published on Marriott's website on September 23, 2016, October 5, 2017, and September 19, 2019. *Id.* The allegedly false or misleading portions of these statements are as follows:

##### Security

***We seek to use reasonable organizational, technical and administrative measures to protect Personal Information within our organization.*** Unfortunately, no data transmission or storage system can be guaranteed to be 100% secure. If you have reason to believe that your interaction with us is no longer secure (for example, if

you feel that the security of your account has been compromised), please immediately notify us in accordance with the “Contacting Us” section below.

¶ 498 (September 23, 2016, Marriott’s Privacy Statement).

#### SAFE HARBOR

In addition, Starwood is certified under the Safe Harbor privacy framework as set forth by the U.S. Department of Commerce, European Commission and Switzerland regarding the collection, storage, use, transfer and other processing of PII transferred from the European Economic Area or Switzerland to the U.S. Please note that since October 6, 2015, the European Union no longer recognizes Safe Harbor. ***Nonetheless, Starwood upholds to comply with the Safe Harbor Privacy Principles.***

#### DELETION AND RETENTION OF YOUR PERSONAL DATA

***Your personal data will be kept in a form which enables [sic] to identify you for no longer than it is necessary for the purposes for which we collected and use your data.*** Your personal data may be retained in certain files for a period of time as required by applicable law and following Starwood’s data retention policies in order to comply with such financial or legal requirements, to properly resolve disputes or to troubleshoot problems. In addition, some types of information may be stored indefinitely due to technical constraints, and will be blocked from further processing for purposes which are not mandatory by law.

\*\*\*

#### SECURITY SAFEGUARDS

***Starwood recognizes the importance of information security, and is constantly reviewing and enhancing our technical, physical, and logical security rules and procedures. All Starwood owned web sites and servers have security measures in place to help protect your personal data against accidental, loss, misuse, unlawful or unauthorized access, disclosure, or alteration while under our control. Although “guaranteed security” does not exist either on or off the Internet, we safeguard your information using appropriate administrative, procedural and technical safeguards, including password controls, “firewalls” and the use of up to 256-bit encryption based on a Class 3 Digital Certificate issued by VeriSign, Inc. This allows for the use of Secure Sockets Layer (SSL), an encryption method used to help protect your data from interception and hacking while in transit.***

¶ 534 (October 5, 2017, Privacy Statement).

#### Security

***We seek to use reasonable organizational, technical and administrative measures to protect Personal Data.*** Unfortunately, no data transmission or storage system can be guaranteed to be 100% secure. If you have reason to believe that your interaction with us is no longer secure (for example, if you feel that the security of

your account has been compromised), please immediately notify us in accordance with the "Contacting Us" section, below.

**Privacy Shield Certified**

***Marriott International, Inc. and certain of its U.S. affiliates have certified to the EU-U.S. and Swiss-U.S. Privacy Shield frameworks.*** Our certifications can be found at: [www.privacyshield.gov/list](http://www.privacyshield.gov/list). For more information about the Privacy Shield principles, please visit: [www.privacyshield.gov](http://www.privacyshield.gov). Our Privacy Shield Guest Privacy Policy can be found [here](#).

¶ 571 (September 19, 2018, Marriott's Global Privacy Statement).

Plaintiff alleges that these statements were false and misleading because at the time they were made, Starwood's IT systems were severely vulnerable, and the statements gave investors "a false impression that Marriott was operating the newly-acquired Starwood systems in accordance with relevant requirements, standards, and best practices" and "a false impression that Marriott had made adequate preparations and dedicated adequate resources to cybersecurity." *See* ¶¶ 499–500, 535, 572–73. In addition, Plaintiff alleges the latter two privacy statements were false and misleading because when warning of cybersecurity risks, Defendants failed to disclose critical facts relevant to those risks "including the vulnerability of the customer data and that the Data Breach was currently ongoing" and that Marriott was in violation of the Safe Harbor Principles and Privacy Shield Frameworks. ¶¶ 535, 572. Finally, Plaintiff alleges that the last privacy statement was false and misleading because Marriott had actual knowledge of the data breach at the time. ¶ 572.

Plaintiff fails to allege facts to plausibly infer that these statements were false or misleading. To begin with, Marriott did not guarantee that customer data would be protected. To the contrary, each of the privacy statements contained a disclaimer that data protection could not be guaranteed. ¶¶ 498, 571 ("[N]o data transmission or storage system can be guaranteed to be 100% secure."); ¶ 534 ("'[G]uaranteed security' does not exist either on or off the Internet."). In

addition, the first and third privacy statements state that Marriott “seek[s] to use reasonable” measures to protect customers’ data. While Plaintiff alleges what it views as deficiencies in Marriott’s cybersecurity, Plaintiff’s allegations do not support the inference that Defendants did not *seek* to protect customer data with reasonable measures. Moreover, where Starwood listed specific measures that it would take to protect customer data, “including password controls, ‘firewalls’ and the use of up to 256-bit encryption based on a Class 3 Digital Certificate issued by VeriSign, Inc.,” there are no allegations that this was not done.

Plaintiff’s allegations that Marriott violated the Safe Harbor and Privacy Shield frameworks also fail to plausibly show that the privacy statements were material misrepresentations at the time they were made. The Safe Harbor and Privacy Shield frameworks are a set of principles that preceded the GDPR regarding EU data protection laws. ¶¶ 409–11. The Safe Harbor Framework was in effect until 2015 and was designed to assist U.S. companies that process personal data that is collected in the EU with complying with European privacy regulations. *Id.* at ¶ 410. The E.U.-U.S. Privacy Shield Framework became effective in 2016 and the Swiss-U.S. Privacy Shield Framework became effective in 2017. *Id.* at ¶ 411. Both were designed to guide American and European companies in complying with European data privacy requirements when transmitting customer data from Europe to the U.S. *Id.* The Safe Harbor and Privacy Shield frameworks each consist of seven similar principles for companies to certify compliance: (1) provide individuals notice regarding the collection and use of their data; (2) provide individuals a choice regarding how the company uses the individual’s data; (3) transfer data to a third party only if they have complied with the first two requirements; (4) take reasonable measures to secure personal data; (5) use data only for the purpose it was collected; (6) provide individuals with access to the individual’s personal data; and (7) have mechanisms in place to

enforce these requirements and remedy problems that arise in the context of the frameworks. *Id.* at ¶¶ 410–11.

Plaintiff alleges that Marriott was in violation of these principles based on findings from the PFI report that Starwood’s systems allowed for insecure remote access, had insufficient logging and monitoring of firewall activity and remote access, and payment cards were stored from October 2002 to December 2018. ¶ 412. But once again, Plaintiff does not get the benefit of hindsight to turn Marriott’s privacy statements into false statements at the time they were made based on the findings of the PFI report. *In re Under Armour Sec. Litig.*, 342 F. Supp. 3d at 677 (no benefit of 20/20 hindsight). This is particularly true given that Plaintiff fails to plead that any of the Defendants authored or were aware of the contents of the privacy statements.

Plaintiff’s allegation that the last privacy statement was false or misleading because Defendants allegedly were aware of the data breach also fails. The last privacy statement was made on September 19, 2018. ¶ 571. As previously discussed, Plaintiff alleges that on September 7, 2018, the IBM Guardium database alert tool discovered the data breach. ¶ 255. On September 10, 2019, Marriot brought in a third-party investigator, Crowdstrike, to perform a review of the hacked systems. *Id.* By September 17, 2018, Crowdstrike determined that attackers had installed webshells, VPN tools, and malware on Starwood’s systems, including a RAT. ¶ 255. The Board was notified of this information by September 18, 2018. *Id.* It was not until November 19, 2018 that Marriott learned that encrypted files were removed that contained guests’ personal information. Thus, the Board was aware that a cyber-attack had occurred before its September 19, 2018 privacy statement, but not the extent of the attack or that customer information had been compromised. These allegations do not support the inference that Defendants made a false or misleading statement by stating, “We seek to use reasonable organizational, technical and

administrative measures to protect Personal Data.” This is especially true when in the very next sentence Marriott stated it could not provide a 100% guarantee that personal data could not be compromised.

Defendants also argue that the privacy statements do not meet Section 10(b)’s “in connection with” requirement because they were not made in connection with the purchase or sale of a security. “The Supreme Court has consistently embraced an expansive reading of § 10(b)’s ‘in connection with’ requirement.” *U.S. S.E.C. v. Pirate Inv’r LLC*, 580 F.3d 233, 244 (4th Cir. 2009) (quoting *SEC v. Wolfson*, 539 F.3d 1249, 1262 (10th Cir. 2008)). Fraudulent activity satisfies the in connection with requirement “whenever it ‘touches’ or ‘coincides’ with a securities transaction.” *Id.* (citing *Merrill Lynch, Pierce, Fenner & Smith, Inc. v. Dabit*, 547 U.S. 71, 85 (2006)); *see also* *Superintendent of Ins. of N.Y. v. Bankers Life & Cas. Co.*, 404 U.S. 6, 12–13 (1971) (holding “in connection with” requirement satisfied where injury occurred “as a result of deceptive practices touching [a] sale of securities”).

To determine whether an alleged fraud touches or coincides with a securities transaction to satisfy Section 10(b)’s “in connection with” requirement, the Fourth Circuit has considered four factors:

- (1) whether a securities sale was necessary to the completion of the fraudulent scheme, *S.E.C. v. Zandford*, 535 U.S. 813, 820–21 (2002);
- (2) whether the parties’ relationship was such that it would necessarily involve trading in securities, *Rowinski v. Salomon Smith Barney Inc.*, 398 F.3d 294, 302–03 (3d Cir. 2005);
- (3) whether the defendant intended to induce a securities transaction, *United Int’l Holdings, Inc. v. Wharf (Holdings) Ltd.*, 210 F.3d 1207, 1221 (10th Cir. 2000), *aff’d*, 532 U.S. 588 (2001); and
- (4) whether material misrepresentations were “disseminated to the public in a medium upon which a reasonable investor would rely,” *Semerenko v. Cendant Corp.*, 223 F.3d 165, 176 (3d Cir. 2000).

*U.S. S.E.C. v. Pirate Inv'r LLC*, 580 F.3d at 244–45. This is not an exclusive set of factors, and an alleged fraud need not satisfy every factor in order to meet the “in connection with” requirement. *Id.* Rather, these factors guide the inquiry to “help distinguish between fraud in the securities industry and common law fraud that happens to involve securities.” *Id.* (citing *Zandford*, 535 U.S. at 820).

Here the parties focus on the fourth factor: whether the privacy statements were disseminated in a public medium in a way in which a reasonable investor would rely. This standard is derived from a Second Circuit opinion, *SEC v. Texas Gulf Sulphur Co.*, 401 F.2d 833 (2d Cir. 1968) (en banc). The *Texas Gulf* standard has since been refined and employed by other circuits, including the Fourth Circuit, as follows:

Where the fraud alleged involves public dissemination in a document such as a press release, annual report, investment prospectus or other such document on which an investor would presumably rely, the “in connection with” requirement is generally met by proof of the means of dissemination and the materiality of the misrepresentation or omission.

*U.S. S.E.C. v. Pirate Inv'r LLC*, 580 F.3d at 249 (quoting *Rana Research, Inc.*, 8 F.3d at 1362; citing *Wolfson*, 539 F.3d at 1262; *Semerenko*, 223 F.3d at 176.). This standard has been applied to, for example, investment research reports from a reputable broker, prospectuses, sales and marketing materials at brokerage houses and other points of sale, SEC filings, and detailed drug advertisements published in sophisticated medical journals. *Id.* at 250 (collecting cases). As the Fourth Circuit explained, “[a]t its core, the *Texas Gulf* standard is about notice—attaching liability under the securities laws for statements made in any medium, no matter how tangentially related to the securities markets, would run the risk of roping in speakers who had no idea that their conduct might implicate Section 10(b).” In other words, “by requiring that misstatements be communicated in a medium upon which a *reasonable* investor would rely, the *Texas Gulf* standard

protects these unknowing speakers from liability and ensures that there is a sufficient nexus between the misrepresentations and the securities sales that they induce to satisfy the Supreme Court's command that the fraud and securities sales 'coincide.'" *Id.* at 250–51.

The question here is whether reasonable investors would rely on Marriott's privacy statements on its website to create a sufficient nexus between the alleged misrepresentations in the privacy statements and the purchase of securities.

Defendants answer no, pointing to *In re LifeLock, Inc. Sec. Litig.*, 690 F. App'x 947, 953–54 (9th Cir. 2017). In that case, the Ninth Circuit held that advertisements describing LifeLock's membership benefits for identity theft protection and comparing its services to other forms of credit monitoring and credit card protection, as well as a statement on its website that it takes "fast action" to alert its subscribers to possible identity theft, were not probative of securities fraud. *In re LifeLock, Inc. Sec. Litig.*, 690 F. App'x at 953–54. The Ninth Circuit noted that "[t]hese three ads might have some probative value in an action based on consumer protection laws, but they have none in a case alleging investor fraud." *Id.*

Plaintiff disagrees and cites *Equifax*, in which the court found that a statement on Equifax's website that it "takes great care to ensure that we use and process personal data in ways that comply with applicable regulations and respects individual privacy," along with similar statements, were actionable under Section 10(b). *In re Equifax Inc. Sec. Litig.*, 357 F. Supp. 3d at 1227. The court, however, did not discuss Section 10(b)'s "in connection with" requirement when making this determination. *See id.* In other cases, statements posted to a website were found to be actionable. *See S.E.C. v. Enterprises Sols., Inc.*, 142 F. Supp. 2d 561, 577 (S.D.N.Y. 2001); *S.E.C. v. StratoComm Corp.*, 2 F. Supp. 3d 240, 259 (N.D.N.Y. 2014).

Although I am skeptical that Plaintiff's allegations support the inference that a reasonable investor would rely on Marriott's privacy statements when purchasing securities, I need not reach this conclusion as a matter of law. Rather, for the reasons discussed above, Plaintiff fails to allege facts to plausibly infer that the privacy statements themselves were false or misleading to a reasonable investor. Because Plaintiff fails to allege that the privacy statements are false or misleading, it also fails to allege that they contain material omissions. *Matrixx Initiatives, Inc. v. Siracusano*, 563 U.S. at 44 ("Disclosure is required under [Section 10(b) and Rule 10b-5] only when necessary 'to make . . . statements made, in the light of the circumstances under which they were made, not misleading.'") (quoting 17 CFR § 240.10b-5(b)).

#### **vi. SOX Certifications**

Plaintiff alleges that certifications Mr. Sorenson and Ms. Oberg signed under the Sarbanes-Oxley Act of 2002 ("SOX") were false and misleading because they certified the risk factor disclosures. ¶¶ 462, 487, 496, 507, 517, 524, 532, 541, 555, 562, 569, 589. These disclosures state, for example:

*I have reviewed this annual report on Form 10-K of Marriott International, Inc.; Based on my knowledge, this report does not contain any untrue statement of a material fact or omit to state a material fact necessary to make the statements made, in light of the circumstances under which such statements were made, not misleading with respect to the period covered by this report. . . .*

¶ 462. Because neither the risk factor disclosures nor other statements identified by Plaintiff in Marriott's SEC filings were false or misleading or contained material omissions, Plaintiff's allegations regarding the SOX certifications fail.

#### **b. Scienter**

Plaintiff's claims must be dismissed for a second reason: even assuming that Defendants made material misrepresentations or omissions, Plaintiff fails to adequately allege scienter. To meet the scienter requirement for a Section 10(b) and Rule 10b-5 claim, a plaintiff "must show

that the defendant acted with ‘a mental state embracing intent to deceive, manipulate, or defraud.’” *Zak v. Chelsea Therapeutics Int'l Ltd.*, 780 F.3d 597, 606 (4th Cir. 2015) (*quoting Tellabs v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 319 (2007)). In the Fourth Circuit, “a plaintiff must allege that the defendant made the misleading statement or omission intentionally or with ‘severe recklessness’ regarding the danger of deceiving the plaintiff . . . A showing of mere negligence will not suffice.” *Teachers' Ret. Sys. of LA v. Hunter*, 477 F.3d 162, 183–84 (4th Cir. 2007) (*quoting Ottmann v. Hanger Orthopedic Group, Inc.*, 353 F.3d 338, 343–44 (4th Cir. 2003) (internal citation omitted)). To meet the level of recklessness required under this standard, an act must be “‘so highly unreasonable and such an extreme departure from the standard of ordinary care as to present a danger of misleading the plaintiff to the extent that the danger was either known to the defendant or so obvious that the defendant must have been aware of it.’” *Matrix Cap. Mgmt. Fund, LP v. BearingPoint, Inc.*, 576 F.3d 172, 181 (4th Cir. 2009) (*quoting Pub. Employees' Ret. Ass'n of Colo. v. Deloitte & Touche LLP*, 551 F.3d 305, 313 (4th Cir. 2009)); *see also Lerner v. Nw. Biotherapeutics*, 273 F. Supp. 3d 573, 594 (D. Md. 2017).

The PSLRA heightened the requirements for pleading scienter. Whereas Federal Rule of Civil Procedure 9(b) only requires a person’s state of mind to “be alleged generally,” the PSLRA requires a plaintiff to allege particularized facts leading to a “strong inference” of scienter. 15 U.S.C. § 78u-4(b)(2). To qualify as strong, “an inference of scienter must be more than merely plausible or reasonable—it must be cogent and at least as compelling as any opposing inference of nonfraudulent intent.” *Tellabs*, 551 U.S. at 314. This requires a court to “engage in a comparative evaluation; it must consider, not only inferences urged by the plaintiff . . . but also competing inferences rationally drawn from the facts alleged.” *Id.* The evaluation must be holistic, considering “whether *all* of the facts alleged, taken collectively, give rise to a strong inference of

scienter, not whether any individual allegation, scrutinized in isolation, meets that standard.” *Id.* at 323 (emphasis in original). “[T]he inference of scienter must be more than merely ‘reasonable’ or ‘permissible’—it must be cogent and compelling, thus strong in light of other explanations.” *Id.* at 324. Therefore, a complaint will survive “only if a reasonable person would deem the inference of scienter cogent and at least as compelling as any opposing inference one could draw from the facts alleged.” *Id.* This pleading requirement applies to the state of mind of *each* of the Individual Defendants. *See Teachers’ Ret. Sys. of LA v. Hunter*, 477 F.3d at 183–84. Because Defendant Marriott is a corporation, Plaintiff “must allege facts that support a strong inference of scienter with respect to at least one authorized agent of the corporation, since corporate liability derives from the actions of its agents.” *Id.* For forward-looking statements, the required level of scienter is “actual knowledge.” 15 U.S.C. § 78u–5(c)(1)(B); *see Matrixx Initiatives, Inc. v. Siracusano*, 563 U.S. at 48 n.14.

Here Plaintiff argues that a strong inference of scienter is established through confidential witness allegations, internal documents during and after the breach was discovered, violations of data security standards, Defendants’ involvement in the merger, and the magnitude of the breach. Examining each of these allegations and considering them holistically with opposing inferences demonstrates that Plaintiff fails to plead a strong inference of scienter for any of the Defendants.

### **i. Confidential Witness Allegations**

Plaintiff includes in its complaint statements from seven confidential witnesses who were former employees of Marriott or Starwood. “When the complaint chooses to rely on facts provided by confidential sources, it must describe the sources with sufficient particularity to support the probability that a person in the position occupied by the source would possess the information alleged or in the alternative provide some other evidence to support their allegations.” *Teachers’*

*Ret.*, 477 F.3d at 174 (internal citation and quotation marks omitted). However, “[o]missions and ambiguities count against’ an inference of scienter because a complaint’s factual allegations must be stated with particularity.” *Yates v. Mun. Mortg. & Equity, LLC*, 744 F.3d at 885–86 (quoting *Tellabs*, 551 U.S. at 326). And “courts should steeply discount allegations from confidential sources that lack sufficient indicia of reliability.” *Id.* (*citing Institutional Investors Grp. v. Avaya, Inc.*, 564 F.3d 242, 263 (3d Cir. 2009)). Here Plaintiff describes the position, period of employment, responsibilities, and supervisors for each confidential witness. I find the allegations regarding the confidential witnesses as credible and, for the purposes of this motion, consider them to be true.

The confidential witness allegations largely focus on the sufficiency of Marriott’s cybersecurity. For example, Confidential Witness 1 (“CW 1”), a Software Developer and Technical Lead employed by Marriott from May 2005 to March 2018, stated that it was apparent to some that Starwood did not invest in its IT equipment because it was old. ¶¶ 64, 156. Confidential Witness 2 (“CW 2”), a Senior Global Cyber-Security Consultant employed by Starwood from September 2014 to December 2015, stated that Starwood used an antiquated version of the Oracle application portal. ¶¶ 13, 65. The Oracle Application portal is a web-based application that enables users to access content areas, external websites, and other applications including the Starwood Reservation and SPG Loyalty Points systems. ¶¶ 13, 154. CW 2 stated that Starwood did not pay Oracle for support so updates or patches to prevent hacking were not implemented. This left the Oracle portal seven years past its end of life. *Id.* Further, CW 2 stated that customer user and employee user IDs and passwords were stored in Starwood databases “in the free and clear” and the passwords were not encrypted. ¶ 159. According to CW 2, Starwood was not properly providing security log monitoring for its more than 800 servers, Starwood lacked

Privilege Access Management (“PAM”) tools to store application and database service account credentials, and Starwood’s IT security staff of about five people at the time was insufficient to protect against vulnerabilities and incidents. ¶¶ 14, 160, 161, 169.

The Confidential Witnesses also described the integration of Starwood and Marriott’s systems. CW 1 said that he did not think anyone at Marriott appreciated how long the integration would take. ¶ 209. Confidential Witness 6 (“CW 6”), a Director of Network Services employed by Marriott from February 2014 to March 2018, stated that Marriott’s existing system could not handle the IT integration, and that Marriott did not forecast the costs of the integration or they were greater than expected. ¶¶ 69, 191. He said that because the IT integration was more expensive than anticipated, increased budgets for IT integration were presented to the board. ¶¶ 216–17.

But some of the Confidential Witness allegations show that Marriott did invest in elements of its cybersecurity. CW 1 stated that “Marriott invested a lot of resources into the tokenization process” with their customers’ credit card information. ¶ 171. Though here Plaintiff points out that while Marriott invested in tokenization, Starwood had no tokenization at all. *Id.* Confidential Witness 5, (“CW 5”), a Senior Director at Marriott’s corporate headquarters from the start of the Class Period through early 2017, stated that the due diligence process was “extremely detailed” and ultimately the decision was made to dispose of almost all of Starwood’s system with the “sole exception” of Starwood’s loyalty rewards system, which they wanted to migrate, because Marriott’s IT leadership believed there was a high likelihood of threat. ¶¶ 175–80.

In large part the Confidential Witnesses criticized Marriott’s IT decisions and the allegations suggest that they would have made different decisions regarding Marriott’s cybersecurity. For example, Starwood used Symantec for its Security Incident Event Management

(“SIEM”) process, which collects and aggregates log data for Starwood’s servers. CW 2 did not believe this was sufficient and recommended IBM’s SIEM tool instead. ¶¶ 160–61. CW 2 also stated that he recommended that Starwood implement an Identity Access Management system to secure their applications and databases and PAM Service Accounts, but instead of spending \$10 to \$20 million for a new system roll out, Starwood chose a quicker and cheaper option called “salted hash” to encrypt user passwords. ¶ 165. CW 2 stated that, at best, salted hash would just slow down rather than stop attackers and hackers from gaining access to passwords. *Id.* CW 1 said that Marriott did not have enough money to invest in IT security because they spent so much on the acquisition, and that Marriott frequently would pull resources from other teams to assist with IT security. ¶¶ 207, 210. At the same time, CW 1 said that Marriott made the decision to purchase “ridiculously expensive” hardware that CW 1 believed was not needed for the IT integration. ¶ 208. CW 1 said that 99% of the IT decisions at Marriott came down to a financial expense consideration. ¶¶ 211–12.

Along this same theme, CW 6 stated that the project to integrate Starwood’s IT systems into Marriott was in three phases. The first phase, while bidding for Starwood was ongoing, consisted of Virtual Private Network tunnels, which were low-cost, encrypted connections that allowed Starwood to send information to Marriott. The second phase involved building circuits between Starwood and Marriott’s data centers to transfer data. To do so, CW 6 said that Starwood and Marriott chose a lower-cost, higher-risk option over a higher-cost, more secure option. Phase 3 involved firewalling Starwood’s systems. Marriott built firewalls around almost all of Starwood’s properties, but not its data centers. CW 6 described this as a compromise approach. CW 6 also described a change in culture as different IT leadership took charge of the project during these phases. ¶¶ 194–99.

None of the Confidential Witness allegations are regarding Defendants deceiving investors. Besides CW 5, who reported to Mr. Hofmeister, none of the Confidential Witnesses reported to the Defendants. And none of the Confidential Witness allegations are regarding what any of the Individual Defendants actually knew about Marriott's cybersecurity or the falsity of any statements.

Some of the Confidential Witnesses speculate about what the Individual Defendants or Marriott as an entity may have known. CW 1 stated that he believes Marriott's senior executives should have seen or been aware of weaknesses in Starwood's systems because they were so old and that he did not see how Marriott's senior executives could not have known because replacing IT hardware was a capital expenditure that would have to be approved by senior management. ¶ 183. CW 6 said that Starwood told Marriott that Starwood's IT security was inferior to Marriott's. ¶ 191. CW 5 stated that the primary reason that Starwood was looking to be acquired was that its Oracle application portal was beyond being patched and would cost hundreds of millions of dollars to fix and that Marriott knew this. ¶¶ 15, 153. CW 5 also stated that as part of the leadership team, he participated in various team meetings in which "all the senior technical leadership participated" and that Marriott was aware of Starwood's security flaws before, during, and after the acquisition. ¶¶ 19, 175, 176. Confidential Witness 7 ("CW 7"), a Director of Engineering/IT at one of Marriott's overseas locations, stated that he was on a conference call in late 2016 or early 2017 soon after Starwood was acquired, in which Mr. Hoffmeister allegedly communicated that Marriott did not have a strong strategy to merge the Starwood and Marriott systems within the declared deadline of end of 2018, but that the target date was going to be met no matter what. ¶¶ 70, 206.

Taken together, these Confidential Witness allegations support the inference that Starwood had cybersecurity deficiencies. The allegations also support an inference that individuals at

Marriott were aware of various deficiencies, but fall short of an inference that the Individual Defendants were aware of any specific deficiency. While some of the allegations support the inference that Marriott did not adequately address Starwood's cybersecurity deficiencies, the allegations also support the inference that Marriott was spending significant time and resources conducting due diligence and investing in cybersecurity, even if the ultimate decisions were not the same as would be made by the Confidential Witnesses. None of the allegations are regarding any allegedly false or misleading statements that Defendants made or demonstrate that Defendants made any statements with actual knowledge or reckless disregard that any statements were false or misleading. Thus, the Confidential Witness allegations fail to support a strong inference of scienter for any of the Defendants.

## **ii. Internal Documents**

Plaintiff argues that Marriott's internal documents support a strong inference of scienter. First, Plaintiff points to several cybersecurity assessments that were completed while the breach was occurring. In March 2016, Pricewaterhouse Coopers ("PwC") conducted a "penetration test" of Marriott's systems and was able to successfully gain access to them. CW 1 stated that these findings were presented to the Board, including the Audit Committee and Mr. Sorenson and Mr. Hoffmeister. ¶ 215.

A Marriott internal report from July 18, 2016, titled, "Marriott IT Infrastructure & Security Business Cases" described several cybersecurity risks with Starwood's systems. Specifically, the report stated that Starwood did not have a SIEM process in place to monitor IT security events for the guest reservation database; Starwood did not monitor and report on the company's state of security; Starwood did not have visibility on malware on its out-of-date systems; and Starwood did not use tokenization or point-to-point encryption on its systems. ¶ 219.

After the merger closed, Marriott commissioned PwC to conduct a “Starwood Cybersecurity Assessment,” which was presented to the Board at the February 10, 2017 Board meeting. PwC found vulnerabilities in Starwood’s systems including: lack of an “enterprise-wide security governing body directing strategic and tactical decisions based on business need;” lack of adequate network segmentation that could allow malicious actors to move from a single, initial point of entry to other data-storing systems; (3) non-compliance or deviations from configuration standards, including that Starwood’s brand standards did not mandate PCI compliance; and (4) that Starwood’s cybersecurity practices had “not reached the maturity level expected from an organization that fits Starwood’s risk profile.” ¶ 220, 314–15.

Later in 2017, Marriott commissioned PwC to provide an assessment of the integration up to that point. PwC advised Marriott that the combined network needed upgrades and to develop an Enhanced Security Administrative environment to lock down and isolate privileged accounts to only authorized individuals. ¶ 221.

In 2018, Marriott commissioned the consulting firm Protiviti to perform a penetration test of Starwood’s system holding payment card data. Protiviti found “19 critical or high priority vulnerabilities, 32 medium, and 28 low priority issues.” Protiviti was also able to capture domain administrator credentials and as a result “Protiviti was in complete control of the Starwood networks.” ¶ 222–23.

These allegations support the inference that Defendants were aware of cybersecurity deficiencies in Marriott’s systems. But they also support an inference that Marriott was taking cybersecurity seriously, actively commissioning assessments and audits of Marriott’s and Starwood’s systems. These assessments do not support the inference that Defendants were aware

of or ignored the data breach, which was already underway by the time these reports were commissioned and was not identified by any of the cybersecurity audits.

Plaintiff also points to unseen documents that were cited in the complaint filed in the Delaware Chancery Court discussed above. According to Marriott's Board Minutes from August 7, 2014, Mr. Sorenson and other board members discussed recently publicized data breach incidents, including the Target data breach, and received a presentation titled "Security Overview" detailing recent cybersecurity incidents at other companies. ¶ 302. Plaintiff goes on to cite the Delaware Chancery Court plaintiffs' statement that nonetheless the board failed to retain the services of an outside analyst or consultant to audit any cybersecurity risks Starwood brought to the merger. ¶ 302. But as just described, the Plaintiff's own complaint in this case contradicts this statement, detailing several cybersecurity assessments commissioned by Marriott.

Marriott's Board minutes from February 12, 2016 indicate that Ms. Oberg gave a presentation on risks facing Marriott to the Board, which showed that the Board ranked cybersecurity as the number one risk facing Marriott in 2016. ¶ 305. At the February 8, 2017 Audit Committee meeting, the Audit Committee was informed by its consultant Ernst & Young about the increased risk of cybersecurity and that the Audit Committee was expected to understand the business implications of cyber risks and the appropriateness of Marriott's cybersecurity risk disclosures required by the SEC. ¶ 310. During the February 10, 2017 Board meeting, the Board ranked cybersecurity as the second biggest risk facing Marriott in 2017 and stated that continuous efforts to identify and mitigate risks were required. ¶ 311. The Board also received a presentation titled, "Marriott Cybersecurity Report," which showed 51 hospitality companies, including HEI, Mandarin, Hilton, and Starwood, had experienced data breaches in the last several years. ¶ 313.

Like the allegations regarding Marriott's cybersecurity assessments, these allegations support the inference that Defendants were aware of cybersecurity deficiencies in Marriott's systems. But here again they also support an inference that Marriott was taking cybersecurity seriously, with its Board ranking cybersecurity as a top risk facing the company and commissioning several audits of Marriott's IT systems. None of the allegations are regarding any allegedly false or misleading statements that Defendants made or demonstrate that Defendants made any statements with actual knowledge or reckless disregard that any statements were false or misleading. Thus, the Marriott internal documents fail to support a strong inference of scienter for any of the Defendants.

### **iii. Cybersecurity “Red Flags”**

Plaintiff alleges that various cybersecurity “red flags” throughout the class period support a strong inference of scienter. *See ¶¶ 611–14.* First, Plaintiff points to several incidents apart from the data breach in which RAM-scraper malware, a type of malware that searches for strings of data that look like credit card numbers and saves them to a text file for exfiltration, was found on Starwood systems. ¶¶ 341, 611. Specifically, RAM-scraper malware was found on Starwood systems on November 20, 2015, five days after the merger was announced. ¶ 361. Starwood stated that this breach was contained by Starwood prior to the merger announcement and Marriott stated that it was aware of the breach. ¶ 362. RAM-scraper malware was also found in Starwood systems in November 2016, two months after the close of the merger. ¶ 363. And during Verizon’s forensic investigation following the data breach, it discovered evidence of additional installation and execution of RAM-scraper malware between December 31, 2016 and January 20, 2017, and between January 9, 2017 and October 19, 2018. ¶¶ 364–65. Plaintiff alleges that had Marriott

installed a proper malware detection system, it would have discovered at least one aspect of the data breach within two months of closing instead of two years later. ¶ 366.

Second, Plaintiff points to cybersecurity incidents that happened at other companies, including other hospitality companies. ¶ 612. Specifically, Plaintiff alleges that there were at least twelve breaches of companies in the hospitality industry involving payment card data and/or personal information, and, as noted above, during the February 10, 2017 Board meeting, Mr. Sorenson and the Audit Committee were presented with information on more than 50 data breaches in 2015 and 2016. *Id.* Plaintiffs allege this should have put Defendants on notice of the heightened risk of a potential data breach.

Plaintiff alleges that these past breaches of Starwood's systems and cybersecurity incidents at other companies put Defendants on notice of the heightened risk of a data breach at Starwood, and this supports a strong inference of scienter. ¶ 614. These allegations do support an inference that Defendants should have been aware of the risk of a cyber-attack on Starwood's systems. But these allegations do not support an inference that any of Defendants' statements were made with knowledge or with reckless disregard that they were false or misleading. To the contrary, as discussed above, Marriott repeatedly disclosed that it was at risk of a cyber-attack. *See, e.g.,* ¶¶ 485, 494, 505. And none of the other statements alleged to be false or misleading suggests the contrary. Therefore, these allegations do not support a strong inference of scienter.

#### **iv. Alleged Violations of Data Security Standards**

Plaintiff alleges that Defendants' violations of data security standards based on the PFI report support a strong inference of scienter. ¶ 599. The PFI report is a summary of Verizon's forensic investigation following the data breach. ¶¶ 330–31. Plaintiff includes a detailed summary of the findings of the PFI report and attaches the report to its Complaint. *See* ¶¶ 330–80; ECF No.

609-1. At its core, Plaintiff alleges that the PFI report found four conditions that existed at the time of the attack that enabled the intrusion, or contributed to the effects of the intrusion:

- (1) Starwood's system allowed for insecure remote access, meaning the network itself was not protected from simple attacks;
- (2) Starwood either lacked or had insufficient access/query and firewall logging, which meant there was insufficient, or a lack of, data for Starwood or Marriott to monitor;
- (3) Starwood lacked monitoring and logging of remote access, meaning that there was no one assigned to monitor who was accessing the systems; and
- (4) Starwood inadvertently stored payment account numbers on systems and in databases that were not designated for the storage of payment account numbers, which meant that Starwood was leaving sensitive data exposed for attackers to access.

¶ 335.

Plaintiff alleges that the findings of the PFI Report show that Marriott was in violation of multiple data security standards. First, Plaintiff alleges that Marriott violated PCI DSS standards. ¶¶ 367–70. The PCI DSS standards are the information security standards for organizations that handle branded credit cards from the major credit card companies, which Marriott was subject to as a credit card payment merchant and processor. ¶ 104. Plaintiff alleges that Marriott violated PCI DSS requirements to “(1) restrict traffic from untrusted networks and hosts; (2) render cardholder data unreadable anywhere it is stored; (3) secure administrative and remote access with multi-factor authentication; and (4) implement automated audit trails for actions taken by users with root or administrative privileges.” ¶ 368.

Second, Plaintiff alleges that Marriott violated principles of the Internal Control-Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (the “COSO Framework”). ¶¶ 389–98. Plaintiff states that Marriott claimed that it used the COSO framework to evaluate the effectiveness of its internal controls on its Form 10-k filings. ¶ 389.

Plaintiff alleges that the COSO Framework requires Marriott to assess risks, create an information and communication system, establish monitoring activities, and establish a system of internal controls. ¶¶ 390–95. Plaintiff alleges that they failed to meet these standards and most significantly failed to identify and assess changes that could significantly impact the Company’s systems and were severely reckless in failing to develop control activities over technology to achieve the Company’s business objectives. *Id.*

Third, Plaintiff alleges that Marriott violated the Federal Trade Commission (“FTC”) Act and the National Institute of Standards and Technology Cybersecurity Framework (“NIST-CSF”) standards. ¶¶ 399–404. Section 5 of the FTC Act requires corporations to refrain from unfair or deceptive trade practices. I previously held that the Consumer Plaintiffs adequately alleged that Section 5 of the FTC Act imposed a duty on Marriott to protect its customers’ personal identifying information in a separate track of this MDL. *See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 478–82 (D. Md. 2020). Here Plaintiff alleges that the contours of this duty include the 2015 FTC Guide, *Start with Security*, the FTC’s 2015 settlement with Wyndham Hotels regarding three separate data breaches it suffered, and the NIST-CSF standards, which were endorsed by the FTC in 2017 as a good source of fundamental security practices. ¶¶ 399–401. Plaintiff argues that Marriot violated the FTC Act and these standards based on the PFI report’s observations, including that Marriott had insecure remote access, insufficient logging of firewall activity, insufficient monitoring and logging of remote access activity, and storage of payment account numbers and card data in clear text. ¶¶ 399, 404.

Fourth, Plaintiff alleges that Marriott violated requirements of the EU’s GDPR. ¶¶ 405–08. Plaintiff cites a notice by the United Kingdom’s Information Commissioner’s Office, an independent authority that enforces the GDPR, that it intends to fine Marriott for violating the

GDPR and failing to perform adequate due diligence during the merger. ¶ 405. Plaintiff alleges that Marriott violated the GDPR by the PFI Report's observations that Marriott had insecure remote access, insufficient logging of firewall activity, insufficient monitoring and logging of remote access activity, and storage of payment account numbers and card data in clear text. ¶ 408.

Fifth, Plaintiff alleges Marriott violated the U.S.-EU Safe Harbor Framework and the EU-U.S. Privacy Framework and the Swiss-U.S. Privacy Shield Framework. ¶¶ 409–12. Plaintiff alleges that Starwood stated on its website that its data security practices were in compliance with the U.S.-EU Safe Harbor Framework and Marriott stated on its website that it followed the Privacy Shield Frameworks. ¶ 409. As discussed above, these frameworks were predecessors to the EU's GDPR and were designed to assist U.S. companies in complying with European privacy regulations. ¶¶ 409–11. Once again, Plaintiff alleges that Marriott violated these standards by the PFI Report's observations that Marriott had insecure remote access, insufficient logging of firewall activity, insufficient monitoring and logging of remote access activity, storage of payment account numbers and card data in clear text, and storage of some payment card information for more than sixteen years. ¶ 412.

Finally, Plaintiff alleges that Marriott was in violation of best practices as described in several articles regarding data security published in the journal of The Information Systems Audit and Control Association ("ISACA"). ¶¶ 413–21 (citing Bostjan Delak & Marko Bajec, *Conducting IS Due Diligence in a Structured Model Within a Short Period of Time*, ISACA J. Volume 4 (2014); Jeimy J. Cano, *Cyberinsurance—The Challenge of Transferring Failure in a Digital, Globalized World*, ISACA J. Volume 5 (2015); Vipin Arora, Deepak Khazanchi, *Evaluating IT Integration Risk Prior to Mergers & Acquisitions*, ISACA J. Volume 2 (2016)). Plaintiff alleges that these articles provide exemplars for how due diligence should have been

conducted, including that the CEO should be accountable for the Information Security due diligence process, the CIO should be responsible for conducting the due diligence, and that the due diligence process should properly evaluate business risks including cybersecurity. ¶¶ 414–20. Plaintiff alleges that Marriott failed to meet these exemplar practices by failing to properly assess and mitigate the risk to Marriott in operating Starwood’s systems, failing to adequately protect customers’ personal data, and failing to adequately monitor and log firewall activity and remote access. ¶¶ 417–19.

Taken together, Plaintiff pleads that these alleged violations of cybersecurity standards and the findings of the PFI Report support a strong inference of scienter. Specifically, Plaintiff alleges that these failures constitute a knowing or severely reckless disregard for the true state of Starwood’s systems by Defendants when they made statements and omitted information to the market. ¶¶ 598–602.

The allegations support an inference that Starwood’s cybersecurity was deficient and failed to meet various cybersecurity standards and best practices. But the findings of the PFI report, including that Marriott had insecure remote access, insufficient logging of firewall activity, insufficient monitoring and logging of remote access activity, and storage of payment account numbers and card data in clear text, which Plaintiff repeatedly cites to support its allegations that Marriott violated various cybersecurity standards, say nothing at all about any of the individual Defendants or what they knew at the time the allegedly false or misleading statements were made. Just as Plaintiff cannot allege that a statement was false or misleading based on hindsight, it cannot plead scienter by hindsight. *Cf. Doshi v. Gen. Cable Corp.*, 823 F.3d 1032, 1044 (6th Cir. 2016) (allegations that “[h]ad the defendants properly used the COSO framework . . . they would have known about accounting errors” on a timely basis “amount to impermissible fraud by hindsight”

and “cannot give rise to a strong inference of scienter.”). Therefore, these allegations fail to support a strong inference of scienter for any of the Defendants.

#### **v. Magnitude of the Breach**

Plaintiff alleges that the size, scope, and duration of the data breach support a strong inference of scienter. ¶¶ 320–25, 617–20. The PFI report found that the data breach went undetected for more than 1,500 days, including more than 700 days while under Marriott’s ownership and control. ¶ 617. The attackers used 17 different accounts to steal the personal information of 380 million people. ¶¶ 617–20. Plaintiff refers to the data breach as the second largest data breach in history. ¶ 618. Plaintiff pleads that these allegations support a strong inference of scienter. ¶ 620.

The scope and duration of the data breach do not support an inference that Defendants knew of the data breach, though it could support an inference that they should have known sooner. However, Plaintiff’s allegations also support the inference that the attackers effectively and intentionally concealed the hack, as neither Marriott nor its outside experts and consultants which, as Plaintiff alleges, conducted multiple cybersecurity assessments, identified the breach sooner. Therefore, these allegations do not support a strong inference of scienter. *See In re Constellation Energy Grp., Inc. Sec. Litig.*, No. CIV. CCB-08-02854, 2012 WL 1067651, at \*7 (“[C]alling a problem ‘long-standing’ does not necessarily suggest that knowledge of the problem was long-standing, and knowledge is the ultimate touchstone for the purpose of determining recklessness.”).

#### **vi. Defendants’ Positions and Involvement in Merger**

Finally, Plaintiff alleges the positions and backgrounds of the Individual Defendants support a strong inference of scienter. ¶¶ 621–33. Plaintiff alleges that Mr. Sorenson, as CEO and a member of the Board, was personally involved in the merger. ¶ 621. Mr. Sorenson had numerous

meetings with Starwood executives and Marriott's Board to stay informed about the merger process. *Id.* According to the best practices in one of the ISACA publications, Plaintiff also alleges that as CEO, Mr. Sorenson should have been intimately involved with the due diligence process. *Id.* Further, Plaintiff alleges that Mr. Sorenson was known to be "hands on" regarding Marriott's merger activity and formerly was a mergers and acquisitions partner with Latham & Watkins. ¶ 623. Plaintiff alleges that this information provides further evidence that Mr. Sorenson knew or was at least severely reckless in not knowing about Starwood's cybersecurity deficiencies and risks. ¶¶ 622–23.

Plaintiff alleges that Ms. Oberg, as CFO, presented to the board three times during the class period regarding cybersecurity risks. ¶ 624. In addition, by virtue of her role, Plaintiff alleges that Ms. Oberg would have been informed regarding the decision to perform information security due diligence and reported the results to the board. ¶ 625. Plaintiff also alleges that as a member of the Board and Marriott's senior management, Marriott was aware of cybersecurity risks facing Marriott. ¶ 626. Plaintiff alleges that this information provides further evidence that Ms. Oberg knew or was at least severely reckless in not knowing about Starwood's cybersecurity deficiencies and risks. ¶¶ 624–26.

For Mr. Hoffmeister, Plaintiff alleges that as CIO, he was deeply involved in the merger and integration process. ¶ 629. And as CIO, Mr. Hoffmeister was responsible for overseeing the people, processes, and technologies within Marriott's IT organization and preserving Marriott's digital assets. ¶¶ 630–32. Plaintiff alleges that this supports a strong inference of scienter. ¶ 632.

Plaintiff alleges Mr. Bauduin, as CAO and signatory of Marriott's Form 10-Qs, 10Ks, and 8-Ks, was responsible for reviewing the statements in those filings. ¶ 633. As such, he would

have been involved in or informed of the due diligence and integration process, and was also named a manager of Starwood at the end of the merger. *Id.*

Plaintiff does not plead separate allegations of scienter for Defendants Bush, Henderson, Kellner, Muñoz, and Lewis, but addresses them collectively as members of the Audit Committee. ¶¶ 627–28. As members of the Audit Committee, Plaintiff alleges that these Defendants were provided with information regarding the deficiencies in Starwood’s systems, were aware of their responsibilities to disclose risks regarding cybersecurity, and had actual knowledge of the breach ten weeks before it was disclosed to the public. *Id.*

Finally, Plaintiff alleges that as a corporation, Marriott acted with scienter by virtue of the scienter of the Individual Defendants, and the statements of other company officials. ¶ 634.

I consider these allegations as part of my holistic assessment. *See Yates v. Mun. Mortg. & Equity, LLC*, 744 F.3d at 890. These allegations support an inference that the Individual Defendants should have known that Starwood’s systems had cybersecurity deficiencies. But without “additional detailed allegations” regarding the Individual Defendants, they do not establish an inference, let alone a strong one, that any of the Individual Defendants knew or was reckless in not knowing that any of their statements were false or misleading. *Id.*; *see also Lerner v. Nw. Biotherapeutics*, 273 F. Supp. 3d at 593–94 (collecting cases and noting, “Courts have routinely held that corporate executives’ access to information and internal affairs is not enough to demonstrate scienter under the PSLRA.”)

#### **vii. Countervailing Inferences of Innocence**

In addition to weighing the inferences above, I must also consider countervailing inferences of innocence from the Complaint. *Yates v. Mun. Mortg. & Equity, LLC*, 744 F.3d at 885.

First, Defendants argue that Plaintiff's failure to plead any plausible fraudulent motive or insider stock sales weighs against a finding of scienter. The absence of an alleged motive is not fatal to a complaint. *Tellabs*, 551 U.S. at 325. Nonetheless, courts have considered the lack of motive as a relevant circumstance. For example, in *Sgarlata v. PayPal Holdings, Inc.*, the Northern District of California found that the lack of an alleged motive cut against an inference of scienter in connection with a data breach of a Paypal-owned company. 409 F. Supp. 3d 846, 859 (N.D. Cal. 2019). The court explained:

The weakness of any inference of scienter is underscored by the lack of any obvious incentive to mislead. There is no allegation of motivation – e.g., that Defendants sold stock during the Class Period or that any of the individual defendants stood to gain a profit from the alleged wrongdoing. Nor is there any satisfying explanation of what benefit Defendants hoped to gain by delay[ing] disclosure of the full scope of the breach by three weeks. This was not like overestimating financial performance of a company with the hope and possibility that financial fortunes might improve and thereby mask an otherwise misleading statement. If there were a breach causing 1.6 million customer files to be compromised, that fact could not be undone, mooted, or masked by waiting three weeks.

*Id.* The district court's dismissal and reliance on a lack of alleged motive was affirmed by the Ninth Circuit. *Eckert v. PayPal Holdings, Inc.*, 831 F. App'x 366, 367 (9th Cir. 2020). *See also In re Acterna Corp. Sec. Litig.*, 378 F. Supp. 2d 561, 577 (D. Md. 2005) ("[T]he absence of any allegations establishing a motive for the individual Defendants to engage in securities fraud cuts against Plaintiffs' argument."). Here Plaintiff does not allege that any of the Individual Defendants sold stock in Marriott or had any other motive for making false or misleading statements. While not dispositive, this weighs against an inference of scienter.

Second, Defendants point out that Plaintiff's allegations show that Marriott launched an immediate investigation when it was alerted to suspicious inquiries. ¶ 354. This also weighs against an inference of scienter. *See Higginbotham v. Baxter Int'l, Inc.*, 495 F.3d 753, 758 (7th

Cir. 2007) (launching investigation after data breach “demonstrat[es] a pursuit of truth rather than reckless indifference to the truth.”)

Similarly, the Complaint states that Marriott reported the breach to the FBI, including “the tools used by the hackers, the timeliness of the intrusion, and the forensic findings the Company and/or its third-party investigators had made.” ¶35. Working cooperatively with law enforcement supports an inference that the Defendants were not simultaneously perpetuating a scheme to deceive investors. *Cf. In re Bausch & Lomb, Inc. Sec. Litig.*, 592 F. Supp. 2d 323, 342–43 (W.D.N.Y. 2008) (no inference of scienter when company “immediately launched a massive independent investigation” into accounting irregularities and “voluntarily reported the matter to the SEC.”)

Finally, Defendants point to Marriott’s repeated disclosures that it could be subject to a cyberattack. *See, e.g.*, ¶¶ 485, 494, 505. These disclosures informed investors that Marriott may not be able to keep up with information, security, and privacy requirements and it was not impervious to cyberattacks. *Id.* This weighs against an inference of scienter that the Individual Defendants were intentional or severely reckless in leading investors to believe the opposite.

#### **viii. The Court’s Prior Decision in the Consumer Track**

For each alleged false statement, Plaintiff states that I already held in a separate track of this MDL that the Consumer Plaintiffs adequately pleaded under Fed. R. Civ. P. 9 “that Marriott knew or should have known about allegedly inadequate security practices and risk of a data breach.” *See, e.g.*, ¶445. Plaintiff argues that this holding should sustain its claims here. Pl. Opp. at 16.

In a prior Memorandum Opinion regarding Marriott’s motion to dismiss the claims filed by the Consumer Plaintiffs, I found that the Maryland and California class representatives

adequately pled violations of the Maryland Consumer Protection Act and California Unfair Competition Law Claims, respectively. *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d at 489. These statutes protect consumers with respect to their purchase of goods and services. I explained that Rule 9(b) required the Consumer Plaintiffs to allege the time, place, and contents of false representations regarding their purchase of goods and services, but that Rule 9(b)'s requirements are applied less strictly with respect to omissions. The Consumer Plaintiffs met this requirement with respect to their claims under these statutes by alleging that they gave their personal information to Marriott and their allegations that Marriott knew or should have known that the personal information was not secure.

In contrast, the pleading requirements of the PSLRA are substantially more demanding than those of Rule 9(b), as discussed above.<sup>7</sup> See Section I.b. The PSLRA requires the Plaintiff to plead specific facts to support the inference that Defendants made material representations or omissions to investors. For the reasons discussed above, Plaintiff has failed to adequately plead that any of the alleged statements identified in the Complaint were false or misleading. Moreover, the PSLRA's heightened scienter requirement was not applicable to the claims by the Consumer Plaintiffs. And for the reasons stated above, Plaintiff here has failed to adequately plead scienter. My analysis of a different complaint, by different plaintiffs, alleging different statutory violations, under different standards, does not change this result.

## ix. Holistic Assessment

Each of the categories of allegations discussed above fails to support a strong inference of scienter. The sum of the parts is no different. Plaintiff's allegations based on confidential

---

<sup>7</sup> Federal Rule of Civil Procedure 9(b) states: "In alleging fraud or mistake, a party must state with particularity the circumstances constituting fraud or mistake. *Malice, intent, knowledge, and other conditions of a person's mind may be alleged generally.*" (emphasis added).

witnesses, internal cybersecurity assessments and board minutes, the PFI report and various data security standards, and the magnitude of the breach all support an inference that Marriott's cybersecurity was deficient. The allegations also demonstrate that the Individual Defendants were aware of cybersecurity risks. But the allegations also support the opposing inference that Marriott conducted due diligence and made investments in its IT infrastructure, even if they were not the same decisions that some of the confidential witnesses would have made. The lack of an alleged motive, investigation into the data breach, cooperating with law enforcement, and disclosure of the risk of a cyber-attack all support an inference of innocence. Taken together, Plaintiff fails to allege a strong inference that Defendants acted with an intent to deceive or with severe recklessness to the truth. Because “the facts as a whole more plausibly suggest that the defendant acted innocently—or even negligently—rather than with intent or severe recklessness, the action must be dismissed.” *Cozzarelli v. Inspire Pharm. Inc.*, 549 F.3d 618, 624 (4th Cir. 2008).

### **c. Loss Causation**

Defendants argue that Plaintiff fails to adequately plead the loss causation element of a claim under Exchange Act Section 10b and Rule 10b-5. Allegations of loss causation are reviewed for “‘sufficient specificity,’ a standard largely consonant with Fed. R. Civ. P. 9(b)’s requirement that averments of fraud be pled with particularity.” *Katyle v. Penn Nat. Gaming, Inc.*, 637 F.3d 462, 471 (4th Cir. 2011); *see also Singer v. Reali*, 883 F.3d 425, 444–45 (4th Cir. 2018).<sup>8</sup> This

---

<sup>8</sup> In *Katyle v. Penn Nat. Gaming*, the Fourth Circuit explained that in *Tellabs*, the Supreme Court recognized that “[p]rior to the enactment of the PSLRA, the sufficiency of a complaint for securities fraud was governed not by [the general pleading standard of] Rule 8, but by the heightened pleading standard set forth in Rule 9(b).” *Katyle v. Penn Nat. Gaming, Inc.*, 637 F.3d 462, 471 n.5 (4th Cir. 2011) (quoting *Tellabs*, 551 U.S. at 319). As described above, the PSLRA sets forth specific standards for pleading the elements of misrepresentation and scienter that supersede the requirements of Rule 9(b), but it does not address the pleading standards applicable to the remaining elements of a § 10(b) claim, “and so presumably the pleading standard of Rule 9(b) still applies to those elements.” *Id.* The Fourth Circuit recognized that uncertainty has arisen because in *Dura Pharm., Inc. v. Broudo*, 544 U.S. 336, 346–47

“requires the pleading of ‘a sufficiently direct relationship between the plaintiff’s economic loss and the defendant’s fraudulent conduct,’ which may be accomplished by alleging facts establishing that the defendant’s ‘misrepresentation or omission was one substantial cause of the investment’s decline in value.’” *Singer v. Reali*, 883 F.3d at 445 (quoting *Katyle v. Penn Nat. Gaming, Inc.*, 637 F.3d at 472). “[T]he plaintiff must plead (1) the ‘exposure’ of the defendant’s misrepresentation or omission, i.e., the revelation of ‘new facts suggesting [the defendant] perpetrated a fraud on the market,’ and (2) that such exposure ‘resulted in the decline of [the defendant’s] share price.’” *Singer v. Reali*, 883 F.3d at 445 (quoting *Katyle v. Penn Nat. Gaming, Inc.*, 637 F.3d at 43).

Plaintiff may allege exposure for the purposes of loss causation under the “corrective disclosure” theory, the “materialization of concealed risk” theory, or a combination of the two. *Id.* “[U]nder the corrective disclosure theory, a complaint may allege that the defendant company itself made a disclosure that ‘publicly revealed for the first time’ that the company perpetrated a fraud on the market by way of a material misrepresentation or omission.” *Id.* (citing *Katyle*, 637 F.3d at 473). “[U]tilizing the materialization of a concealed risk theory, a complaint may allege that news from another source revealed the company’s fraud.” *Id.* (citing *Katyle*, 637 F.3d at 477 n.10.) “In such a case, the plaintiffs would not need to identify a public disclosure that corrected the previous, misleading disclosure because the news of the materialized risk would itself be the revelation of the fraud that caused plaintiffs’ loss.” *Katyle*, 637 F.3d at 477 n.10 (quoting *Teachers’ Ret. Sys.*, 477 F.3d at 187). In *Singer*, the Fourth Circuit found that an “amalgam” of

---

(2005), the Supreme Court applied Rule 8’s “a short and plain statement” pleading standard to allegations of loss causation, but had simply assumed for argument’s sake that that standard applied. *Id.* Therefore, the Fourth Circuit applies the “sufficient specificity” standard consonant with Rule 9(b) to allegations of loss causation. See *id.*; *Singer v. Reali*, 883 F.3d 425, 444–45 (4th Cir. 2018).

the two theories was sufficient to plead exposure for the purposes of loss causation. *Singer v. Reali*, 883 F.3d at 445.

Under any of these theories of exposure, “the ultimate loss causation inquiry . . . is the same: whether a ‘misstatement or omission concealed something from the market that, when disclosed, negatively affected the value of the security.’” *Id.* at 446 (quoting *In re Vivendi, S.A. Sec. Litig.*, 838 F.3d 223, 261–62 (2d Cir. 2016)). In other words, a plaintiff must show “that the loss caused by the alleged fraud results from the ‘relevant truth . . . leak[ing] out.’” *Id.* (quoting *In re Vivendi, S.A. Sec. Litig.*, 838 F.3d at 261; *Dura Pharm., Inc. v. Broudo*, 544 U.S. at 342).

For corrective disclosures, “neither a single complete disclosure nor a fact-for-fact disclosure of the relevant truth to the market is a necessary prerequisite to establishing loss causation (although either may be sufficient).” *Id.* (quoting *Katyle*, 637 F.3d at 472). Instead, “the truth may have ‘gradually emerged through a series of partial disclosures,’ with the ‘entire series of partial disclosures [prompting] the stock price deflation.’” *Id.* (quoting (quoting *Katyle*, 637 F.3d at 472) (alterations in original)). The disclosure or series of disclosures “‘need not precisely identify the misrepresentation or omission’ about which the plaintiff complains, but ‘must reveal to the market in some sense the fraudulent nature of’ such misrepresentation or omission, and ‘must at least relate back to the misrepresentation [or omission] and not to some other negative information about the company.’” *Id.* (quoting *Katyle*, 637 F.3d at 473) (alterations in original).

Here Plaintiff alleges that Marriott’s November 30, 2018 announcement of the data breach was a “corrective disclosure and/or revelation of a previously concealed, materialized risk” that caused Marriott’s share price to drop by \$6.81 from a close of \$121.84 per share on November 29, 2018 to \$115.03 per share on November 30, 2018, and that this caused Plaintiff and other class members economic losses. ¶¶ 635–43. But for the reasons discussed above, Plaintiff has failed to

allege that Defendants made any material false statements or omissions. Therefore, the disclosure of the data breach necessarily did not correct or reveal a previous misstatement or omission. In other words, with no misrepresentation or omission, Plaintiff cannot show that its alleged losses “relate back to [a] misrepresentation and not to some other negative information about the company.” *Katyle v. Penn Nat. Gaming, Inc.*, 637 F.3d at 473. Thus, Plaintiff fails to allege loss causation.

## **II. Secondary Liability Under Exchange Act Section 20(a)**

In the second count of the Complaint, Plaintiff alleges secondary liability under Exchange Act Section 20(a). ¶¶ 664–72. Section 20(a) states:

Every person who directly or indirectly, controls any person liable under any provision of this chapter or of any rule or regulation thereunder shall also be liable jointly and severally with and to the same extent as such controlled person to any person to whom such controlled person is liable . . . unless the controlling person acted in good faith and did not directly or indirectly induce the act or acts constituting the violation or cause of action.

15 U.S.C. § 78t(a). “A ‘claim for controlling person liability under section 20(a) must be based upon a primary violation of the securities laws.’” *Lerner v. Nw. Biotherapeutics*, 273 F. Supp. 3d at 596 (quoting *Svezzese v. Duratek, Inc.*, 67 Fed. Appx. 169, 174 (4th Cir. 2003)). Here the alleged predicate violations for Section 20(a) liability are the alleged violations of Exchange Act Section 10b and Rule 10b-5 discussed above. ¶ 666. Because Plaintiff fails to state a claim under Exchange Act Section 10b and Rule 10b-5, its claim under Exchange Act 20(a) fails as well.

## **III. Dismissal with Prejudice**

For the reasons stated above, Plaintiff’s claims are dismissed. This dismissal is with prejudice. “The determination whether to dismiss with or without prejudice under Rule 12(b)(6) is within the discretion of the district court.” *Weigel v. Maryland*, 950 F. Supp. 2d 811, 825–26 (D. Md. 2013) (quoting *180S, Inc. v. Gordini U.S.A., Inc.*, 602 F. Supp. 2d 635, 638–39 (D. Md.

2009)). Generally, when there has been no opportunity to amend, the dismissal should be without prejudice and the plaintiff granted an opportunity to amend. *See Adams v. Sw. Va. Reg'l Jail Auth.*, 524 F. App'x 899, 900 (4th Cir. 2013) ("Where no opportunity is given to amend the complaint, the dismissal should generally be without prejudice."). Here Plaintiff has already amended three times. *See* ECF Nos. 401 (first amended complaint), 440 (second amended complaint), 609 (third amended complaint). This includes two amendments after Plaintiff had notice of the Defendants' arguments for dismissal. *See* ECF No. 414 (Defendants' pre-motion letter explaining arguments for dismissal). The current complaint spans 674 paragraphs over 317 pages with an additional 211 pages of exhibits. Further amendment would be futile and the claims are dismissed with prejudice.

### **CONCLUSION**

In sum, Defendant's motion to dismiss is granted. Plaintiff has failed to allege a material misrepresentation or omission, a strong inference of scienter, and loss causation. For each of these reasons, the Complaint must be dismissed. Because Plaintiff has already amended its Complaint three times, further amendment would be futile and this dismissal is with prejudice. A separate Order follows.

---

June 11, 2021  
Date

---

/S/  
Paul W. Grimm  
United States District Judge