IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

IN RE: CAPITAL ONE CONSUMER DATA SECURITY BREACH LITIGATION	)	MDL No. 1:19-md-2915 (AJT/JFA)
This Document Relates ONLY to the following case:	)	
EDWARD SHAMOON, individually and on behalf of all others similarly situated,	)	Case No. 1:19-cv-1472 (AJT/JFA)
Plaintiff,	)	
v.	)	
CAPITAL ONE FINANCIAL CORPORATION, *et al*.,	)	
Defendants.	)	

ORDER

Following a data breach pertaining to approximately 100 million consumers, Lead Plaintiff Edward Shamoon, filing on behalf of himself and the purported class of Capital One shareholders, alleges that the Defendants deceived shareholders into buying or retaining Capital One stock by publicly extoling their security program while sacrificing adequate cybersecurity in favor of operational convenience, and as a result, Capital One stock fell in value following disclosure of the breach.[1] *See generally* [Doc. No. 279] ("Am. Compl."). Defendants Richard

[1] On November 2, 2019, a previous lead plaintiff in this case filed a securities fraud action in the Eastern District of New York on behalf of himself and the class of persons who acquired Capital One stock between July 23, 2015 and July 29, 2019. *See generally* 1:19-cv-1472 [Doc. No. 1]. After the action was subsequently converted into a multi-district litigation matter ("MDL") and transferred to this District, *see* [Doc. No. 6-8], an Amended Complaint was filed in this Court on January 17, 2020 and Plaintiff Edward Shamoon was appointed Lead Plaintiff. *See generally* Am. Compl.; [Doc. No. 262] (Order granting Edward Shamoon's motion to be lead plaintiff). In addition to this securities class action, a consumer class action was filed in 2019 related to these same events by the victims of the data breach, which the Judicial Panel on Multi-District Litigation ("JPML") also transferred to this District. *In re:*

Fairbank, Robert Alexander, Michael Johnson (the "Individual Defendants"), and Capital One Financial Corporation ("Capital One") (collectively the "Defendants") have filed a Motion to Dismiss the Amended Class Action Complaint (the "Motion"), [Doc. 318] ("Mot."), for failure to state a claim for relief under Sections 10(b) and 20(a) of the Exchange Act (15 U.S.C. §§78j(b) and 78t(a)) and Rule 10b-5 promulgated thereunder by the SEC (17 C.F.R. § 240.10b-5). The Defendants allege, *inter alia*, that, as a matter of law, the Amended Complaint fails to allege with the required level of particularity why the relied upon misstatements or omissions were materially false or misleading, as well as Defendants' mental state, or scienter, in making the relied upon statements, as required under the heightened pleading standard applicable to securities fraud claims. For the reasons stated below, the Motion is **GRANTED** and this action **DISMISSED**.[2]

I. BACKGROUND

A. Factual Background

Capital One is a bank holding company founded in 1994[3] and headquartered in Virginia. Am. Compl. at ¶¶ 23, 26, 34. Since its inception, Capital One has consistently marketed itself as the most technologically savvy bank and in 2011 embarked on a highly promoted "Digital Transformation" intended to enhance its capabilities related to advertising, credit decisions, and customer service. *Id.* at ¶¶ 2-5. Another important benefit the Digital Transformation offered was enhanced cybersecurity, in part through an automatic encryption program called Cloud Custodian. *Id.* at ¶ 9. As part of the Digital Transformation, Capital One moved most of its data

Capital One Inc. Customer Data Security Breach Litigation, 488 F.Supp.3d 374 (E.D. Va. 2020). The parties in that case agreed to a final settlement which the Court approved on September 8, 2022.

[2] This matter was stayed by Order dated December 21, 2021, which is vacated for the purposes of this ruling. *See* [Doc. No. 2206].

[3] The company was founded as another bank's credit card division and spun off in 1994. *Id.* at ¶ 34.

to the cloud and made Amazon Web Services ("AWS") its predominant cloud provider. *Id.* at ¶ 11. Capital One asserted that the Digital Transformation would make it more effective at securing and maintaining retail partnerships—a significant line of business for it—which would lead to economies of scale. *Id.* at ¶¶ 80-84.

Both before and after the rollout period for the Digital Transformation, the individual Defendants and other Capital One executives made numerous public statements touting the company's approach and procedures related to cybersecurity. *See generally id*. These statements were of several different types, including statements about (1) Capital One's compliance with legal obligations and industry practices generally; (2) compliance with obligations to disclose information about cybersecurity risks in particular; (3) the cybersecurity benefits of the Digital Transformation; (4) the importance of cybersecurity to the company; (5) the encryption of consumer data; and (6) the reasonable length of retention periods and access frequency.[4]

On March 12, 2019, Paige Thompson, a "hacker" acting alone, illegally accessed one of Capital One's cloud-based servers which contained a significant cache of customer data. *Id.* at ¶¶ 171, 173. The data spanned a period of 15 years and implicated a total of 106 million Capital One customers and prospective customers; the data included demographic information, self-reported income, full and partial social security numbers, and wide-ranging credit performance information. *Id.* at ¶¶ 172, 177. While on the server, Thompson obtained summaries of the data and transferred a copy of the data to a storage location outside Capital One's firewall. *Id.* at ¶¶ 174, 179. Thompson's alleged intent in accessing the server was to use Capital One's computing power to mine cryptocurrency (which she did). *Id.* at ¶¶ 181, 187. She did not attempt to

[4] These statements are further discussed *infra* in Section III.A.

publicize or sell the stolen consumer data. *Id.*

Thompson retained access to the server for a protracted period of time, and Capital One was only alerted to the breach on July 17, 2019 by someone who observed Thompson commenting about it in a private chatroom. *Id.* at ¶¶ 181-83. On July 29, 2019, Capital One issued a press release announcing the breach. *Id.* at ¶¶ 189-90. When trading resumed the next day, Capital One's stock fell 5.9% on heavy volume, and the company also suffered widespread criticism, scrutiny, and reputational damage. *Id.* at ¶¶ 190-92. For instance, the month after Capital One's announcement of the breach, the Wall Street Journal published an article citing internal reports of high turnover and discord between staff and senior management. *Id.* at ¶¶ 165-70. Thompson was subsequently prosecuted on charges of wire fraud and computer fraud and abuse.[5] *United States v. Thompson,* Slip Op. #: 2:19-cr-00159-RSL-1 (W.D. Wa., filed July 29, 2019).

According to the Amended Complaint, because machine learning was a key component of the Digital Transformation and because machine learning requires large amounts of data, the company structured its internal data management systems to make data of all types more accessible to its machine learning algorithms. *Id.* at ¶¶ 110-24. Plaintiff alleges numerous deficiencies in Capital One's cybersecurity measures, resulting mainly from some combination of mismanagement and Capital One's desire for operational convenience and machine learning functionality. *Id.* at ¶ 108. Plaintiff primarily alleges cybersecurity deficiencies including over-sized data "lakes," retention of data for unreasonably long periods, failure to tokenize or encrypt data, and an overly lenient practice of granting permissions for its staff to view sensitive data. *See generally id.* Other alleged instances of mismanagement include Capital One's purchase of

[5] It appears from the public record that Thompson was convicted on those charges on June 17, 2022. *See* 2:19-cr-00159-RSL (W.D. Wa.) [Doc. No. 225].

data breach protection software in 2017 that it failed to install for over a year, *id*. at ¶ 170; Capital One's alleged hiring of a Russian third party to illegally purchase stolen consumer data, which it theddn kept on its server in a non-secure, plaintext format, *id*. at ¶¶ 139-40; and Defendant Johnson and his team's dismissal of their staff's concerns, exacerbating attrition and degradation within the cybersecurity division, *see id*. at ¶¶ 138, 150, 166-69. Plaintiff supports these allegations through citations to a combination of trade press stories and information from anonymous former employees. *See generally id.* at ¶¶ 131-70. Overall, Plaintiff alleges that Defendants' false and/or misleading statements regarding cybersecurity induced them, in part, to buy and/or retain Capital One stock, and as a result they were harmed when Capital One's stock price fell 5.9% the day after the announcement of the data breach. *Id*.

The Amended Complaint contains two counts. Count 1 alleges liability under Section 10(b) of the Exchange Act, 15 U.S.C. §78j(b), and SEC Rule 10b-5 against Capital One and all three Individual Defendants: Richard Fairbank, the company's founder and CEO; Robert Alexander, its Chief Information Officer (CIO); and Michael Johnson, its Chief Information Security Officer (CISO) from March through October of 2019 (who was terminated due to the data breach).[6] *Id.* at ¶¶ 27-30, 268-79. Count 2 alleges liability under §20(a) of the Exchange Act, 15 U.S.C. §78j(b), against only the Individual Defendants. *Id*. at ¶¶ 280-84.

On February 18, 2020, the Defendants filed the Motion, [Doc. No. 319], Plaintiff filed an opposition to the Motion on March 10, 2020, and Defendants in turn filed a reply on April 21, 2020. [Doc. No. 345]; [Doc. No. 407].[7] The case has been stayed since December 21, 2021. [Doc. No. 2206].

[6] The Amended Complaint states that Defendant Johnston was terminated in October 2017, but the Court understands this to mean October 2019, i.e. several months after the data breach.
[7] The Motion was originally set for a hearing on March 27, 2020 which was then taken under advisement on March 17, 2020 without a hearing due to the COVID-19 pandemic.

II. LEGAL STANDARDS

Ordinarily, fraud claims are subject to Federal Rule of Civil Procedure 9(b) which imposes an elevated pleading standard whereby a plaintiff must plead with particularity the circumstances constituting fraud or mistake. Fed. R. Civ. Pro. 9(b). However, claims under §10(b) of the Exchange Act, 15 U.S.C. §78j(b) pursuant to SEC Rule 10b-5, as amended by the Private Securities Litigation Reform Act ("PSLRA"), are subject to separate pleading requirements. 15 U.S.C. § 78u-4(b)(1).[8] Congress passed the PSLRA to, among other objectives, unify and raise the pleading standard required to make out a claim for a securities fraud action to reduce abusive and vexatious litigation by private parties. *KBC Asset Mgmt. NV v. DXC Tech. Co.*, 19 F. 4th 601, 607 (4th Cir. 2021).

The PSLRA requires plaintiffs to "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, . . . state with particularity all facts on which that belief is formed." 15 U.S.C. § 78u-4(b)(1). Thus, in evaluating the sufficiency of PSLRA governed pleadings, courts conduct a "statement-by-statement analysis." *In re Genworth Fin. Inc. Sec. Litig.*, 103 F. Supp. 3d 759, 771 (E.D. Va. 2015) (internal citation and quotations omitted).

Some statements are legally incapable of satisfying the material misrepresentation or

[8] "Section 10(b) of the Securities Exchange Act of 1934 forbids the 'use or employ, in connection with the purchase or sale of any security [], [of] any manipulative or deceptive device or contrivance in contravention of such rules and regulations as the [SEC] may prescribe as necessary or appropriate in the public interest or for the protection of investors.'" *Tellabs, Inc. v. Makor Issues & Rts., Ltd.*, 551 U.S. 308, 318 (2007) (quoting 15 U.S.C. § 78j(b)). SEC Rule 10b–5 implements § 10(b) by declaring it unlawful:

> (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 ... 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, in connection with the purchase or sale of any security.

Id. (quoting 17 CFR § 240.10b–5).

omission standard. "'Forward-looking statements' that are either accompanied by cautionary language, immaterial, or made without actual knowledge of their falsity are statutorily protected under the PSLRA's safe harbor provision." *Oklahoma Firefighters Pension & Ret. Sys. v. K12, Inc.*, 66 F. Supp. 3d 711, 714 (E.D. Va. 2014) (citing 15 U.S.C. § 78u–5(c)(1)). Similarly, "puffery," such as generic and rosy statements of corporate optimism, are "not material as a matter of law." *Id.* With respect to puffery, Courts have frequently recognized that there exists:

> [a] certain kind of rosy affirmation commonly heard from corporate managers and familiar to the marketplace—loosely optimistic statements that are so vague, so lacking in specificity, or so clearly constituting the opinions of the speaker, that no reasonable investor could find them important to the total mix of information available.

In re Neustar Sec., 83 F. Supp. 3d 671, 680 (E.D. Va. 2015) (quoting *In re Cable & Wireless, PLC Sec. Litig.*, 321 F. Supp. 2d 749, 766–67 (E.D. Va. 2004)). Whether a statement is puffery tends to answer whether the statement is false or misleading because a true puffing statement by its very nature cannot be materially false or misleading.

In the landmark case *Tellabs*, the Supreme Court defined "scienter," for the purpose of the PSLRA, as "a mental state embracing intent to deceive, manipulate, or defraud." 551 U.S. at 319 (internal quotations and citation omitted). A complaint filed under the PSLRA must state with particularity the facts giving rise to a strong inference of scienter rather than generally as Rule 9(b) allows. *Id.* at 321. This heightened, twice-elevated standard is in excess of both the *Twombley-Iqbal* plausibility standard and Rule 9(b), *id.*, and requires a court to determine 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 322-23 (emphasis in original); *see also Kiken v. Lumber Liquidators Holdings, Inc.*, 155 F. Supp. 3d 593, 606 (E.D. Va. 2015) ("evaluat[ing] the totality of the circumstances alleged in the

complaint" while also "afford[ing] the inferential weight warranted by context and common sense") (internal citation and quotation omitted). In carrying out this analysis, courts must "compare the malicious and innocent inferences cognizable from the facts pled [] and only allow the complaint to survive . . . if the malicious inference is at least as compelling as any opposing innocent inference." *KBC Asset Mgmt.*, 19 F.4th at 608 (internal citation and quotations omitted).

III. ANALYSIS[9]

A securities fraud action must satisfy the following 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 (that is, the economic loss must be proximately caused by the misrepresentation or omission)." *Matrix Capital Mgmt. Fund, LP v. BearingPoint, Inc.*, 576 F.3d 172, 181 (4th Cir. 2009) (emphasis omitted) (quoting *Stoneridge Investment Partners, LLC v. Scientific–Atlanta, Inc.*, 552 U.S. 148, 157 (2008)); *see also In re PEC Sols., Inc. Sec. Litig.*, 418 F.3d 379, 386-87 (4th Cir. 2005) (same). A statement is a "misrepresentation" if "it either (1) is materially false or (2) contains an omission that renders the statement materially misleading." *Oklahoma Firefighters Pension*, 66 F. Supp. 3d at 714 (citations omitted). Whether a misrepresentation or omission is "material" depends on whether "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

[9] Plaintiff has alleged, and Defendants have not disputed, that he purchased Capital One stock during the relevant class period and suffered a loss as a result of the decrease in stock prices following the announcement of the breach (although stock prices later recouped value).

of the fact." *In re PEC*, 418 F.3d at 387 (internal citation and quotations omitted).

Plaintiff generally alleges that Capital One materially misled investors into buying or retaining Capital One stock and inflated the price of that stock when it publicly touted its cybersecurity measures while internally de-emphasizing cybersecurity in favor of machine learning, thereby causing the purported class members' loss when that price fell following the announcement of the data breach. *See generally* Am. Compl. More specifically, Plaintiff alleges that by operating its business with insufficient cybersecurity practices, while misleading investors by their statements regarding those practices, Defendants "engaged in acts, practices and a course of business that operated as a fraud or deceit upon plaintiff and others similarly situated in connection with their purchases of Capital One securities during the class period." Am. Compl. at ¶ 271-c. After viewing the factual allegations most favorably to the Plaintiff, the Court concludes that the Amended Complaint fails to allege securities fraud with the requisite factual support as required under the PSLRA.

A. Material Misrepresentation or Omission

1. Capital One's Legal Obligations and Industry Practices

Plaintiff alleges two material misstatements related to Capital One's Legal Obligations and Industry Practices ("Compliance Statements").

The first, stated on the company's 10-K forms between 2015-2018, as signed by Defendant Fairbank, states in relevant part:

> [W]e continuously evaluate the regulatory environment and proactively adjust our compliance risk program ***to fully address these expectations.*** Our Compliance Management Program . . . regularly monitor[s] and report[s] on the efficacy of their compliance controls and Corporate Compliance.

Am. Compl. at ¶ 208 (emphasis in original). The second is an unattributed statement made on Capital One's website:

> At Capital One, we make your safety and security a top priority and are committed to protecting your personal and financial information. If we collect identifying information from you, ***we will protect that information with controls based upon internationally recognized security standards, regulations, and industry-based best practices***.

Id. at ¶ 210 (emphasis in original). Plaintiff alleges that both statements were false and misleading because Capital One's retention of consumer data ran afoul of, *inter alia*, (1) the FTC recommended protocol and regulation, *id.* at ¶¶ 200-02; and (2) the Payment Card Industry ("PCI") Requirements, which state that companies should "limit[] data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements."[10] *Id.* at ¶¶ 204-06; *see also id.* at ¶ 211.[11]

Both statements constitute immaterial puffery and non-actionable statements of opinion or belief. *See Oklahoma Firefighters Pension*, 66 F. Supp. 3d at 718 (holding "statements [at issue] are the kinds of statements that cannot be objectively demonstrated to be false or misleading"); *see also In re Constellation Energy Grp., Inc. Sec. Litig.*, 738 F. Supp. 2d 614, 631 (D. Md. 2010) (holding a reasonable investor could not assume from general statements about the defendant's "strong risk management culture" and "effective system of internal controls" that they would never lapse in these tasks).

2. Regulatory Obligations to Disclose Information About the Cybersecurity Risks

The Amended Complaint alleges that the cybersecurity risk disclosures given by Capital One in its various 10-K forms were insufficiently tailored to the company's operations, but

[10] Both sets of standards relate more to general compliance objectives than specific and quantitatively-measured compliance outcomes, which makes them a difficult basis upon which to premise a material misstatement or omission. Plaintiff also points to violations of Canadian regulations but this argument is not developed further in the parties' briefing. *See* [Doc. No. 319] (no mention of Canadian regulations in Defendant's memorandum); [Doc. No. 345] (Plaintiff mentions the Canadian regulation only when summarizing the allegations of the Amended Complaint in his opposition); [Doc. No. 407] (no mention in Defendant's reply).

[11] Plaintiff also alleges that these statements ran afoul of customer expectations but provide no further support for that contention. *Id.* at ¶ 211.

instead would apply to any financial services firm or any company with large amounts of consumer data. Am. Compl. at ¶¶ 218, 222. The relied upon statements related to Capital One's warnings of cybersecurity risks appear in the company's 10-K forms from 2015 to 2018. Am. Compl. at ¶ 218; *see generally* [Doc. No. 319-1] at 2.[12] These statements failed, Plaintiff alleges, to disclose that Capital One was sacrificing cybersecurity by pursuing its information-based strategy and that it faced a "particular risk" from granting overbroad access. *Id.* In support of this claim, Plaintiff cites an SEC guidance provision requiring firms to tailor their disclosures in light of particular circumstances (including past incidents such as denial-of-service attacks) and alleges that several "internal breaches" that Capital One previously suffered in Montana necessitated a particularized disclosure of permission-related risks. *Id.* at ¶¶ 219-21.

As an initial matter, the Amended Complaint does not allege with particularity what is false or misleading about the statements provided in the various 10-K forms. [Doc. No. 319-1] at 2; *see In re 2007 Novastar Fin. Inc., Sec. Litig.*, 579 F.3d 878, 882-83 (8th Cir. 2009) (dismissing claims where complaint lacked "any indication as to what specific statements within these communications are alleged to be false or misleading"). Additionally, the relied upon SEC guidance provides that companies "should disclose the risk of cyber incidents if these issues are among *the most significant factors* that make an investment [] speculative or risky" and such disclosures include "discussion of aspects of the registrant's business or operations that give rise to *material* cybersecurity risks and the potential costs and consequences." Am. Compl. at ¶ 212 (emphasis added). Plaintiff fails to allege facts that would establish that cybersecurity breaches in Montana were of such a nature and magnitude that made it "among the most significant

[12] Plaintiff also points to a statement by CFO Richard Blackley stating "obviously, for a financial services firm, making sure that data is secure is a mission critical thing." *Id.* at ¶ 217. This statement is a classic example of puffery that does not qualify as false or misleading.

factors that make an investment [] speculative or risky." With respect to "aspects of the registrant's business or operations that give rise to material cybersecurity risks and the potential costs and consequences," the 10-Ks from which the relied upon statement was taken included pages of disclosures relating to the threat of cybersecurity breaches, which in fact particularized the type of risk associated with the Montana internal breaches (namely, the risk of "fraud or malice on the part of our employees"). Mem. at 17; *see also* [Doc. No. 319-2] at PageID 20-25 (2016 10-K).[13]

3. Digital Transformation Led to Better Cybersecurity

Plaintiff contends that the following six statements are false or misleading concerning how the Digital Transformation would lead to better cybersecurity outcomes.

(1) On Capital One's October 23, 2018 earnings call, Defendant Fairbank stated, in relevant part:

> [W]hat I am struck by [] and I'm not surprised by it, because I believe that that will accelerate here is that ***going all-in on this transformation is the opportunity to be way faster to the market, offer way better products, have way better risk management along credit dimensions, fraud, cybersecurity, that's all a shared path, same thing.*** Better operating controls in a world where the regulatory requirements and frankly the expectations on banks to deliver well-controlled environment in a complex industry is very, very high, better economics, and all of this in service of the most important thing, which is real-time, personalized experience for our customers, not just in an app, but integrated right into their lives. So that's the journey we're on.

Am. Compl. at ¶ 223; [Doc. No. 319-1] at 2 (emphasis in original) (cleaned up).

(2) At the November 30, 2016 JP Morgan FinTech & Specialty Finance Forum, a non-Defendant Capital One executive named Jeff Norris told investors and analysts: "Because of the Digital Transformation, the company was 'also seeing better compliance outcomes.'" Am.

[13] The Montana cyber incidents, which were disclosed through the Montana Department of Justice website, appear to be "one-off instances" committed by employees abusing their authorized access to customer information, rather than the type of "hacker" involved in the 2019 Cybersecurity Breach. *See* Mem. at 17.

Compl. at ¶ 225.

(3) At the June 1, 2017 Sanford C. Bernstein & Co. Strategic Decision Conference, Defendant Fairbank stated that:

> So what we've done over this period of time is to build out the capability of fully digital consumer banking and with a very robust checking account capability, ***all the fraud defenses that go along with digital banking,*** which by the way are significant, because fraudsters by the way don't go walking into local banks. They go set up checking accounts, they like to do all this stuff online.

Id. at ¶ 226.

(4) At the June 15, 2016 Morgan Stanley Financials Conference, Stephen S. Crawford, Capital One's Chief Financial Officer, was listing aspects of Capital One's business that would benefit from the Digital Transformation and included regulatory compliance, stating: "***there's not a single major undertaking or challenge the business has where, if you sit back and think about the implications of being able to deploy to the cloud or big data or open source software, they can't make a huge difference in both the revenue and the expense side.***" Am. Compl. at ¶ 228; [Doc. No. 319-1] at 4 (emphasis in original).

(5) At the December 2, 2015 JP Morgan FinTech & Specialty Finance Forum, CFO Crawford told attendees: "Cyber[security] is an important part of the overall digital process and [] I think as a financial institution trust, the trust of our customers is critical, and we want to make sure that we're a leader in cyber, so it's one of the agenda items we have in the whole digital space." Am. Compl. at ¶ 227; [Doc. No. 319-1] at 3.

(6) On its Schedule 14A Proxy Statement dated March 20, 2018, Capital One stated that their management: "[a]ccelerated focus on cloud capabilities, modern software engineering and delivery, ***and enhanced cybersecurity capabilities***." Am. Compl. at ¶ 229 (emphasis in original).

As an initial matter, Plaintiff has failed to allege with any specificity either when these alleged cybersecurity deficiencies (i.e., "created too many data lakes," "granted access . . . far too easily,") occurred or their scope. Furthermore, all these statements constitute non-actionable forward-looking statements, opinion and/or puffery. *See In re Computer Scis. Corp. Sec. Litig.*, 890 F. Supp. 2d 650, 668 (E.D. Va. 2012) (holding that statements expressing confidence that the defendant company would be awarded a contract fell under PSLRA's safe harbor provision for forward-looking statements, at least with respect to their predictive character); *Neustar*, 83 F. Supp. 3d at 680 ("indefinite statements of corporate optimism" which fail to "demonstrate falsity" are generally non-actionable) (quoting *Carlucci v. Han*, 886 F.Supp.2d 497, 522 (E.D. Va. 2012)). And there are no facts that support the inference that these statements conflicted with opinions the speakers actually held. *See In re Neustar*, 83 F. Supp. 3d at 683 ("In order to plead that an opinion is a false factual statement . . . the complaint must allege that the opinion expressed was different from the opinion actually held by the speaker.") (quoting *Nolte v. Cap. One Fin. Corp.*, 390 F.3d 311, 315 (4th Cir. 2004)).

4. Cybersecurity Was One of Capital One's Top Priorities

Plaintiff has alleged that the following eight statements relating to Capital One's claim that cybersecurity was a priority (the "Priority Statements") are false or misleading:

(1) On the July 23, 2015 earnings call Defendant Fairbank stated: ***"[w]e're investing in cybersecurity. This is an incredibly important area and we are putting a lot of very top talent and a lot of energy and investment into that***." Am. Compl. at ¶ 232 (emphasis in original).

(2) At the October 7, 2015 AWS re:invent conference, Plaintiff alleges that Defendant Alexander stated: "[]***security is critical for us***. The financial services industry attracts some of the worst cyber criminals so we work closely with the Amazon team to develop a security model

that we believe ***enables us to operate more securely in the public cloud than we can even in our own data centers***." Am. Compl. at ¶ 233 (emphasis in original).

(3) At the June 25, 2019 AWS re:inforce conference, Defendant Johnson stated, in relevant part, "***[m]ost important to us is the confidentiality, integrity and the availability of our data in the cloud. Cloud native companies must take a multi-layered approach to security***, leveraging internally developed tools like the Capital One-developed open source Cloud Custodian." *Id.* at ¶ 234 (emphasis in original).

(4) On November 21, 2018, Capital One executive Brady wrote an article appearing on Capital One's website stating in relevant part, "[i]n an effort to help our application teams migrate to the cloud in an unencumbered way, we established a governance function with security and compliance as top considerations." *Id.* at ¶ 235.

(5) Plaintiff also points to Capital One's 2015-2018 10Ks that provide, in relevant part: ***We take measures that mitigate against known attacks and use internal and external resources to scan for vulnerabilities in platforms, systems, and applications necessary for delivering Capital One products and services***. *Id.* at ¶ 236 (emphasis in original).

(6) Capital One's cybersecurity policy states, since September 29, 2018, "[y]our security is a top priority." Am. Compl. at ¶ 238.

(7) Capital One press releases from October 2017, December 2017, and January 2018 quoted non-Defendant Rebecca Hieronimous saying "[w]e know many of our customers actively use the [product at issue] and we are excited to enable this partnership allowing customers to share their data in a way that is ***secure, transparent and under their control***." *Id.* at ¶ 237.

(8) In an August 24, 2018 YouTube video, non-Defendant[14] George Brady stated "[a]s a

[14] The Amended Complaint states that George Brady is a Defendant in this paragraph but this contradicts the earlier section of the Amended Complaint clearly stating that the only Individual Defendants are Fairbank, Alexander, and

financial institution, we take the safety of our customer data incredibly seriously." *Id.* at ¶ 242.

All of these statements constitute non-actionable puffery or forward looking statements.[15] *See In re Ford Motor Co. Sec. Litig.*, *Class Action*, 381 F.3d 563, 570 (6th Cir. 2004) (statements such as "quality [is] a top priority" is "mere corporate puffery or hyperbole that a reasonable investor would not view as significantly changing the general gist of available information" and so is immaterial.). Furthermore, while some of these statements use formal or technical language suggesting a degree of concreteness, they are too vague to cause a reasonable investor to materially rely on them in making an investment decision. *See Raab v. Gen'l Phys. Corp.*, 4 F.3d 286, 289 (4th Cir. 1993) (holding that statements including that the marketplace is poised for continued growth lack materiality because they are too vague to inflate securities price); *see also Carlucci v. Han*, 886 F. Supp. 2d 497, 522 (E.D. Va. 2012) (When puffing statements "are so vague, so lacking in specificity, or so clearly constituting the opinions of the speaker, [then] no reasonable investor could find them important to the total mix of information available.") (internal citation and quotations omitted). And the context of most of these statements—largely business conferences and corporate promotional materials—further underscores that a reasonable investor would not view these kinds of "rosy affirmation[s] commonly heard from corporate managers and familiar to the marketplace" as "important to the total mix of information available." *Neustar*, 83 F. Supp. 3d at 680 (internal quotations and citation omitted); *see also*

Johnson.

[15] Plaintiffs points to a number of other statements that are also immaterial puffery or non-actionable forward-looking statements. *See generally id.* at ¶¶ 241, 243-45. For example, Defendant Fairbank's stated at the Barclays Global Financial Services Conference taking place on September 11, 2017:

> Capital One is trying to build basically a tech company that happens to be a major player in banking and I really think the opportunity is great for players who do that. I think the journey is incredibly hard for banks to get there. The fact that we're regulated, huge capital requirements, the risk management involved in our business and even some of the brand credibility associated with the management of people's private information and their money are things that will help us slow banks possibly make our way successfully to the destination.

Id. at ¶ 241.

Carlucci v. Han, 886 F. Supp. 2d 497, 507 (E.D. Va. 2012) (granting motion to dismiss, in part, because the defendants' statements about high profile investors and "seasoned and highly regarded executives with extensive track records of success" were vague and immaterial and so mere puffery).

5. *Defendants Claimed that the Customer Data It Placed on Its Server was Effectively Encrypted*

Plaintiff alleges Capital One boasted about the efficacy of Capital One's Encryption ("encryption statements"), citing its references to *inter alia*, Cloud Custodian, a product which Capital One stated would "automatically detect and fix security flaws" and "automatically encrypt unencrypted data on Capital One's servers." Am Compl. at ¶¶ 247-49. The particular statements Plaintiff points to include a 2016 statement by Defendant Alexander in a Wall Street Journal's CIO Journal interview, stating in relevant part, "[w]e launched a tool called Cloud Custodian that we built to ensure that we encrypt all data that goes to the cloud . . . . ***If something's not encrypted, it will automatically encrypt it***." Am. Compl. at ¶ 250 (emphasis in original). On June 25, 2019, at the AWS re:inforce conference, Defendant Johnson stated that Capital One's cloud protections include "forced data encryption" in reference to Cloud Custodian. *Id.* at ¶ 251. Also, in each of the company's 10-K forms between 2015 and 2018, signed by Defendant Fairbank, Capital One stated "[w]e believe we have a robust suite of authentication and layered information security controls, including our cyber threat analytics, ***data encryption and tokenization technologies***, anti-malware defenses and vulnerability management program." Am. Compl. at ¶ 252 (emphasis in original). Finally, Capital One's annual privacy notice to credit card holders stated "[t]o protect your personal information from unauthorized access and use, we use security measures that comply with federal law. **These measures include** computer safeguards and **secured files** and buildings." *Id.* at ¶ 253 (emphasis

in original). Plaintiff claims that these statements were false or misleading, as evidenced by its further allegation that "Thompson was assigned credentials that automatically decrypted all the data available in the data lake." Am. Compl. at ¶ 175.

These allegations are sufficiently particular: they allege specifically that Thompson was automatically assigned credentials and did not need to "defeat" an encryption system as Defendants claim. They also facially establish the falsity of Defendants' statements regarding encryption, at least with respect to the stolen data, because an encryption system which grants immediate access even to unauthorized entrants may indeed be aptly described as not meaningfully accomplishing its sole objective. For these reasons, the Amended Complaint sufficiently alleges that these statements were materially false or misleading.

6. Defendants Claimed They Followed Reasonable Access Frequency and Retention Period

Plaintiff alleges two statements related to Capital One's access frequency and retention periods were false or misleading. The first is unattributed, but comes from two press releases issued by the company in late 2017, which claimed that Capital One was "'***[a]ligned with the Consumer Financial Protection Bureau's ["CFPB"] recently released principles***' on data security." Am. Compl. at ¶ 255 (emphasis in original). The Amended Complaint also alleges that a non-defendant Capital One executive, Rebecca Hieronimous, stated in a November 2017 American Banker article: "***[w]e are very aligned with the CFPB principles. As a company, we're 100% focused on ensuring that we have a secure, transparent way for our customers to access their data where they're in control***." Am. Compl. at ¶ 256 (emphasis in original). The statements are comparable to those regarding Capital One's Legal Obligations and Industry Practices, discussed in Section III(A)1, *supra*, and for similar reasons, the Amended Complaint fails to sufficiently allege why these statements are materially false or misleading; they also

constitute non-actionable forward looking statements, opinion or puffery. *See In re Constellation*, 738 F. Supp. 2d at 631 (holding a reasonable investor could not assume from general statements about the defendant's "strong risk management culture" and "effective system of internal controls" that they would never lapse in these tasks). Simply put, stating that "we're 100% focused" is corporate hyperbole a reasonable investor would not interpret to mean 100% of corporate resources were focused on cybersecurity. *See In re Ford*, 381 F.3d at 570. And stating the company is "aligned" with "CFPB principles" is too vague to be actionable. *See Neustar*, 83 F. Supp. 3d at 680.

In sum, the Amended Complaint fails to allege with the required particularity false or misleading statements except those pertaining to the efficacy of its encryption system as described above. *See* Am. Compl. at ¶¶ 250-53.

B. Scienter

"[P]laintiff must allege facts that support a strong inference of scienter with respect to at least one authorized agent of the corporation" and "to the extent a plaintiff alleges fraud claims against individual defendants, the plaintiff must allege facts supporting a strong inference of scienter as to each defendant." *Matrix*, 576 F.3d at 182 (internal citations and quotations omitted). The Amended Complaint fails to sufficiently allege scienter with respect to the falsity or misleading nature of any of the relied upon statements.

Scienter, in the securities fraud context, "refers to a mental state embracing intent to deceive, manipulate, or defraud." *Ottmann v. Hanger Orthopedic Grp., Inc.*, 353 F.3d 338, 343 (4th Cir. 2003) (quoting *Ernst & Ernst v. Hochfelder*, 425 U.S. 185, 194 n.12 (1976)). The PSLRA requires a "Plaintiff to 'state with particularity facts giving rise to a *strong inference*' of scienter." *In re Triangle Cap. Corp. Sec. Litig.*, 988 F.3d 743, 751 (4th Cir. 2021) (quoting 15

U.S.C. § 78u-4(b)(2) (emphasis added)). And the facts must show the defendant made the misleading statements or omissions intentionally or at least with "recklessness," which is defined as being "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." *Ottmann*, 353 F.3d at 343 (citation and internal quotation marks omitted). Relevant to this analysis is also motive for the fraud which, if absent, is not fatal, but can weigh against a finding of the requisite scienter. *Id*.

As mentioned in Section II, *supra*, scienter is a comparative inquiry in which the court must assess whether the strong inference of scienter accompanying the alleged material misrepresentation "is at least as likely as any plausible opposing inference." *Oklahoma Firefighters*, 66 F. Supp. 3d at 715; *see also Tellabs*, 551 U.S. at 322-24. In making that determination, the Court must weigh "the totality of the circumstances alleged in the complaint and afford the 'inferential weight warranted by context and common sense.'" *Kiken v. Lumber Liquidators Holdings, Inc.,* 155 F. Supp. 3d 593, 601-02 (E.D. Va. 2015) (quoting *Carlucci v. Han*, 907 F. Supp. 2d 709, 729 (E.D. Va. 2012)). After considering all the facts alleged collectively, this inquiry asks the court to determine whether a strong inference of scienter arises. *Tellabs*, 551 U.S. at 322-23.

The Amended Complaint alleges that:

> Defendants acted with scienter in that they knew that the public documents and statements issued or disseminated in the name of Capital One were materially false and misleading; knew that such statements or documents would be issued or disseminated to the investing public; and knowingly and substantially participated, or acquiesced in the issuance or dissemination of such statements or documents as primary violations of the securities laws.

Am. Compl. at ¶ 272. Plaintiff alleges that these conclusory allegations are sufficiently

supported "by virtue of [the Individual Defendants'] receipt of information reflecting the true facts of Capital One . . . and/or their associations with the company which made them privy to confidential proprietary information concerning Capital One" as well as based on the Individual Defendants' positions as senior officers/directors. *Id.* at ¶¶ 272-73. More specifically, Plaintiff alleges that the required scienter on the part of Capital One and the Individual Defendants can be reasonably inferred from the reports made by former employee 3 ("FE3") to Defendant Johnson that Capital One's servers experience "upwards of 20 cyber attacks per month," *id.* at ¶¶ 146-50, information which FE3 understands was later reported to Defendant Alexander, *id*., and that Capital One's board "regularly" reviewed the cyber division's attrition rates, *id.* at ¶¶ 167-70. In addition, Plaintiff alleges that several other former employees reported instances of mismanagement to their respective supervisors, but does not allege, even in a conclusory manner, that this information was reported further up the chain of authority. *See generally id*. at ¶¶ 138-45 (allegations related to former employee 2 ("FE 2")).[16]

These conclusory and boilerplate statements with respect to scienter are insufficient to meet the legal standard. Although FE3's allegations tend to show that Defendants Johnson and Alexander had actual knowledge that there were regular cyber attacks, that knowledge does not sufficiently establish that they disbelieved or recklessly made their alleged statements touting Capital One's cybersecurity protocols. Accordingly, scienter cannot be imputed to Johnson, Alexander, or any other Individual Defendant on the basis of these allegations alone. The Amended Complaint alleges only vague statements by Individual Defendants describing the

[16] The Amended Complaint also makes much of FE 2's allegations that Capital One hired a "company closely connected with the Russian government and intelligence agencies [] to illegally purchase [] breached data on the Dark Web." Am. Compl. at ¶¶ 139-44. Plaintiff does not adequately allege, or explain, how, if at all, such allegations relate to the Capital One data breach at issue here as opposed to the Yahhoo! data breach from where the data purportedly came from. To the extent Plaintiff alleges other nefarious practices that compromised data security based on the Russian third party, such allegations are not plead with sufficient detail to support Plaintiff's claims in this action.

significant resources that were dedicated to the digital revolution. *See, e.g.*, Am. Compl. at ¶ 57. But resource allocation cannot reasonably serve as the primary evidence of Defendants' purported actual knowledge of any possible cybersecurity deficiencies. Am. Compl. at ¶ 57.[17]

Similarly, Plaintiff fails to allege sufficient facts that establish scienter with respect to the statements concerning the encryption capabilities of Cloud Custodian, whose false or misleading nature the Court has found adequately pled. *See* Section (III)(A)(5)*, supra.* In that regard, Plaintiff seemingly argues that as executives who dedicated a significant amount of time to the Digital Transformation, the Individual Defendants must have either intentionally or recklessly made false or misleading statements as to Cloud Custodian's capabilities, as illustrated by the Thompson hack. *See, e.g.*, Am. Compl. at ¶¶ 57, 169, 272-73. Such a contention itself is built on the inference that technical aspects of Cloud Custodian and Capital One's cybersecurity protocols must have been elevated, known, and understood at the executive level. But scienter cannot be supported by a foundation of inferences. *See Maguire Fin., LP v. PowerSecure Int'l, Inc.*, 876 F.3d 541, 548 (4th Cir. 2017) ("A plaintiff may not stack inference upon inference to satisfy the PSLRA's pleading standard."); *see also* n.17, *infra.*

Taken together, even if Plaintiff's allegations of Defendants' statements about the Digital Transformation, encryption, and Capital One's cybersecurity priorities were sufficient to establish some degree of mismanagement, Plaintiff fails to establish a strong inference of

[17] Plaintiff also contends that he need not specifically plead any individuals' actual knowledge of Capital One's cybersecurity failings because "the Complaint is premised on the proposition that the Officers directed [them]." [Doc. No 345] at 26. But that conclusory contention is also not plead with the required particularity and would appear inconsistent with certain other allegations. For example, Plaintiff's alleges, in essence, that to the extent there were overly liberal access policies, the practice of granting overbroad access arose among the rank-and-file in response to operational concerns, rather than as a top-down policy driven by Defendants as part of the Digital Transformation. *See, e.g.*, Am. Compl. at ¶ 136 (alleging comments made to the press by a former employee that "[s]etting permissions can be tricky. You may be in a rush to push out code, and if you set permissions that are too narrow, you'll be flooded with troubleshooting requests. So what ends up happening is you set wider permissions and greater access than is necessary.").

intentionality or recklessness by any authorized agent, commensurate with knowing deceit. Plaintiff's allegations more likely support an inference of some level of negligence, which is insufficient to meet the requirements for scienter. *See Cozzarelli v. Inspire Pharms. Inc.*, 549 F.3d 618, 623 (4th Cir. 2008) ("To prove the necessary mental state of scienter, negligence is not enough.").

In short, Plaintiff has failed to allege facts that make Defendants' conduct "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." *Ottmann*, 353 F.3d at 343 (citation and internal quotation marks omitted); *see also Yates v. Mun. Mortg. & Equity, LLC*, 744 F.3d 874, 893 (4th Cir. 2014) (concluding plaintiff failed to establish scienter where "mosaic" of inferences supported "at most[] negligence."). Therefore, the PSLRA's scienter requirement has not been satisfied. [18]

CONCLUSION

Accordingly, for the foregoing reasons, it is hereby

ORDERED that Motion, [Doc. No. 318], be, and the same hereby is, **GRANTED**, sand that this action is hereby **DISMISSED.**

[18] Given the Court's rulings with respect to material falsity and scienter, there is no need for the Court to rule on whether the Amended Complaint has adequately alleged (1) the required connection to the purchase or sale of a security; (2) reliance; or (3) damages and causation.

The Clerk is directed to docket this Order in the lead case (1:19md2915) and the individual case (1:19cv1472), and to forward a copy of the Order to all counsel of record.

/s/
Anthony J. Trenga
United States District Judge

Alexandria, Virginia
September 13, 2022