UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

IN RE EQUIFAX INC. SECURITIES LITIGATION	Consolidated Case No. 1:17-cv-03463-TWT

MEMORANDUM OF LAW IN SUPPORT OF DEFENDANTS' JOINT MOTION TO DISMISS THE CONSOLIDATED CLASS ACTION COMPLAINT

KING & SPALDING LLP
Michael R. Smith
B. Warren Pope
Benjamin Lee
1180 Peachtree Street N.E.
Atlanta, GA 30309

Attorneys for Defendants Equifax Inc., John W. Gamble, Jr., Jeffrey L. Dodge, and Rodolfo O. Ploder

TROUTMAN SANDERS LLP
David M. Chaiken
600 Peachtree Street NE, Suite 3000
Atlanta, GA 30308

QUINN EMANUEL URQUHART & SULLIVAN, LLP
Steven G. Madison (admitted *pro hac vice*)
865 S. Figueroa Street, 10th Floor
Los Angeles, CA 90017

Michael E. Liftik (admitted *pro hac vice*)
Meghan A. McCaffrey (admitted *pro hac vice*)
1300 I Street NW, Suite 900
Washington, D.C. 20005

Attorneys for Defendant Richard F. Smith

TABLE OF AUTHORITIES

Page(s)

Cases

I. INTRODUCTION

On September 7, 2017, Atlanta-based Equifax Inc. ("Equifax" or the "Company")—the parent of one of the three largest credit reporting agencies in the United States—announced that it had been targeted in a criminal cyber attack potentially impacting the personally identifiable information of approximately 143 million U.S. consumers (the "Cybersecurity Incident"). After this announcement, the Company's stock price declined, and, predictably, putative class action lawsuits followed accusing the Company and senior management of securities fraud and seeking recovery of money damages.

Lead Plaintiff Union Asset Management Holding AG's ("Plaintiff") Consolidated Class Action Complaint (the "Complaint"), asserts claims of false and misleading statements under Section 10(b) of the Securities Exchange Act of 1934 (the "Exchange Act") based almost exclusively on hindsight allegations regarding the sufficiency of measures Equifax employed to protect consumer data and guard against an occurrence like the Cybersecurity Incident. As shown below, Plaintiff's allegations fall far short of satisfying the stringent pleading standards imposed by the Private Securities Litigation Reform Act of 1995, 15 U.S.C. § 78u-4 *et seq*. (the "PSLRA").

First, Plaintiff fails to plead a single false or misleading statement of material fact with particularity, as required by the PSLRA. Instead, Plaintiff relies primarily on allegations of purported corporate mismanagement that are not cognizable under Section 10(b), such as allegations that Equifax purportedly failed to implement "adequate" data security protections, including recommendations from consultants. *See, e.g.*, *Santa Fe Indus. v. Green*, 430 U.S. 462, 479-80 (1977) (allegations of mismanagement or the failure to disclose the same are insufficient to plead a Section 10(b) violation). And Plaintiff's allegations fail, in any event, to plead the falsity of Defendants' aspirational statements about Equifax's commitment to data security and statements generally describing the security measures the Company employed.

Courts have dismissed securities fraud claims based on allegations that are indistinguishable in substance from those pled in Plaintiff's Complaint, and this Court should do the same. *See, e.g., In re Heartland Payment Sys., Inc. Sec. Litig.*, 2009 WL 4798148, at *5 (D.N.J. Dec. 7, 2009) (dismissing similar securities fraud claims against transaction card payment processor predicated upon alleged failure to prevent data security breach that resulted in theft of 130 million credit and debit card numbers, remained undetected for a period of time, and triggered an 80% decline in share price upon disclosure); *Ong v. Chipotle Mexican Grill, Inc.*

("*Chipotle II*"), 294 F. Supp. 3d 199, 232 (S.D.N.Y. 2018) (dismissing securities fraud claims against fast food chain predicated on alleged failure to prevent foodborne illness outbreaks due to allegedly inadequate food safety practices).

Second, Plaintiff fails to plead facts which raise the required strong inference of scienter on the part of any Defendant. To adequately plead this element of a securities fraud claim, Plaintiff must allege particular facts establishing that Defendants made false statements with wrongful intent—*i.e.*, "intent to deceive, manipulate, or defraud," or "severe recklessness." *Mizzaro v. Home Depot, Inc.*, 544 F.3d 1230, 1238 (11th Cir. 2008). However, Plaintiff's Complaint is devoid of facts even plausibly suggesting that Defendants were aware of any information contradicting their public statements when made. Instead, Plaintiff's claims hang almost entirely on the unsupported and implausible notion that Defendants knowingly and deliberately failed to patch the software vulnerability at issue in the Cybersecurity Incident—at no conceivable benefit to themselves. Much more plausible is the very explanation Plaintiff pleads, as stated in Mr. Smith's Congressional testimony addressing the Cybersecurity Incident—that unfortunate and unintentional human and system failures contributed to the breach.

Third, the Complaint must be dismissed because Plaintiff fails to adequately plead the element of loss causation, *i.e.*, that the economic losses it claims were

caused by the alleged fraud. *See Dura Pharms., Inc. v. Broudo*, 544 U.S. 336 (2005). To plead loss causation, Plaintiff must tie stock price drops to disclosures of information revealing the falsity of prior statements. *Id.* at 345-48. The Complaint fails to do so. While Plaintiff alleges that Equifax's stock price declined following the public disclosure of the Cybersecurity Incident, Plaintiff has not adequately pled that those price declines were attributable to public revelation of the falsity of any prior actionable misrepresentation by Defendants, rather than to investors reacting to negative information about a criminal theft of data.

For each of these independent reasons, the Complaint should be dismissed.

II. SUMMARY OF ALLEGATIONS AND RELEVANT BACKGROUND

A. Equifax and the Individual Defendants

Equifax is a publicly-traded company whose common stock is listed on the New York Stock Exchange and is the parent of one of the three largest credit reporting agencies in the United States. ¶¶ 19, 363(a).[1] Equifax's U.S. Information Solutions ("USIS") and International business segments provide consumer and commercial credit reporting solutions to businesses in the U.S., Canada, Latin America, Europe, and the Asia Pacific region. ¶ 20; *see also* Ex. A

[1] Cites to "¶ _" refer to paragraphs of the Complaint.

at 2.[2] Equifax's Global Consumer Solutions segment offers consumers in the U.S., Canada, and the U.K. products for monitoring their credit and to help protect their identities. ¶ 20; *see also* Ex. A at 2. Equifax's Workforce Solutions segment consists of two primary business units: (i) Verification Services (offering income and employment verification services) and (ii) Employer Services (offering payroll-related and human resource management solutions). ¶ 20; *see also* Ex. A at 2.

During the putative Class Period, February 25, 2016 through September 15, 2017 (Compl. p.1), Defendant Smith served as Equifax's CEO and Chairman of its Board of Directors (¶ 21); Defendant Gamble served as Equifax's Chief Financial Officer (¶ 22); Defendant Dodge served as Senior Vice President of Investor Relations (¶ 24); and Defendant Ploder served as President of Equifax's Workforce Solutions operating segment (¶ 23). Mr. Smith retired from his positions as Equifax CEO and Board Chairman on September 26, 2017. ¶ 21.

---

[2] Defendants submit as exhibits (cited to herein as "Ex. _") to the Declaration of Benjamin Lee certain SEC filings, press releases, and other public documents that Plaintiff references or purports to partially quote in the Complaint. The Court may take judicial notice of and consider the complete contents of these documents in deciding this motion. *See, e.g., Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 322 (2007).

B. The Cybersecurity Incident

Pertinent allegations and background regarding the Cybersecurity Incident, on which Plaintiff's claims are primarily based, are briefly summarized below.[3]

1. The Apache Struts Vulnerability

In March 2017, a series of public reports were issued warning of a vulnerability in Apache Struts, a software application that is widely used by large businesses to build interactive websites. ¶¶ 95-101. Equifax used Apache Struts to help run a website that enabled consumers to report alleged errors in their credit reports (the "Dispute Portal"). ¶ 95. By March 8, 2017, Apache, the software developer, had released an update "patch" to mitigate the vulnerability. ¶ 98. Equifax had procedures for applying such software patches. *E.g.*, ¶ 103. It also conducted periodic scans of its systems, which were intended to identify similar vulnerabilities. *E.g.*, ¶¶ 104-05. Plaintiff alleges that those procedures (and others) ultimately did not prevent the Cybersecurity Incident. ¶¶ 102-04.

2. Equifax's Investigation of the Cybersecurity Incident

On July 29 and 30, 2017, Equifax security personnel discovered suspicious activity on the Dispute Portal. ¶ 116; Ex. B at 3. The Company acted immediately

[3] These facts are assumed to be true solely for purposes of this motion. *See Tellabs*, 551 U.S. at 2509.

to address the issue and, by July 30, 2017, had taken the Dispute Portal offline. ¶ 102; Ex. B at 3. Plaintiff alleges that the suspicious activity on the Dispute Portal was first reported to Defendant Smith on July 31, 2017. ¶ 118; Ex. B at 3.

On August 2, 2017, Equifax reported the criminal activity to law enforcement and, thereafter, cooperated with the authorities to assist their investigation into the attack. ¶ 120. Also on August 2, 2017, Equifax hired legal counsel to direct an investigation into the attack, and counsel retained the cybersecurity firm Mandiant to assist with the investigation. *Id.* Plaintiff alleges that by August 11, 2017, Mandiant believed that the "hackers may have accessed a database table containing a large amount of consumers' NPPI" (non-public personal information). ¶ 122. Plaintiff alleges that Mr. Smith was informed on August 15, 2017 that "it appeared likely that consumer NPPI had been stolen." *Id.*

Equifax's investigation eventually revealed that, before the unauthorized access was discovered in late July 2017, the hackers were able to access certain Equifax databases and ultimately steal names, Social Security numbers, birth dates, and addresses of potentially as many as 143 million U.S. consumers, as well as certain individuals' driver's license numbers and/or credit card data. ¶ 115. On September 7, 2017, Equifax issued a press release publicly disclosing the

Cybersecurity Incident and its investigative findings as of that date and noting that its investigation remained ongoing. ¶ 124; Ex. C.

C. Plaintiff's Claims and the Challenged Statements

Plaintiff alleges that all Defendants violated Exchange Act Section 10(b) and Rule 10b-5 thereunder by making false and misleading statements to Equifax investors. ¶¶ 373-83. Plaintiff also alleges that the Individual Defendants are liable as "controlling persons" for Equifax's alleged Section 10(b) violations pursuant to Exchange Act Section 20(a). ¶¶ 384-89.

Plaintiff's Complaint challenges approximately thirty statements alleged to have been made by one or more Defendants during the Class Period. ¶¶ 285-353. For the Court's convenience, these challenged statements are identified in a chart attached hereto as Exhibit 1 (the "Statement Chart"). Plaintiff alleges that these statements were false or misleading because Equifax's cybersecurity and data protection measures were "inadequate" and because Equifax "failed to implement" data protection tools and procedures, some of which Plaintiff alleges were recommended to the Company by "security experts," consultants, and others. *See generally* ¶¶ 285-353. Plaintiff also alleges that certain statements that post-date the attack were misleading when made because Defendants knew that the criminals who perpetrated the attack "had penetrated Equifax's internal data systems and

accessed sensitive personal information," but failed to disclose that information. ¶¶ 288, 291, 294, 297, 300, 303, 310, 313-14, 318, 335, 338, 341, 348.

D. Alleged Stock Sales by Defendants Gamble and Ploder

To support allegations of the required element of scienter, Plaintiff alleges that Mr. Gamble sold 13% of his Equifax holdings (equating to roughly one third of his Class Period sales) on August 1, 2017. ¶ 283. Plaintiff also alleges that Mr. Ploder sold 4% of his Equifax holdings (about 20% of his total Class Period sales) on August 2, 2017. *Id.* But Plaintiff does not allege *any* facts establishing that Messrs. Gamble or Ploder knew about the Cybersecurity Incident at the times of their trades; nor does Plaintiff allege *any* stock sales by Mr. Smith or Mr. Dodge.

III. ARGUMENT AND CITATION OF AUTHORITIES

To state a claim under Exchange Act 10(b), Plaintiff must adequately allege "(1) a material misrepresentation or omission; (2) made with scienter; (3) a connection with the purchase or sale of a security; (4) reliance on the misstatement or omission; (5) economic loss; and (6) a causal connection between the material misrepresentation or omission and the loss.'" *Mizzaro*, 544 F.3d at 1236-37.

A. Plaintiff Fails to Plead False or Misleading Statements.

To survive dismissal under the PSLRA's heightened pleading standards, a complaint must "specify each statement alleged to have been misleading [and] the

reason or reasons why the statement is misleading." 15 U.S.C. § 78u-4(b)(1). Plaintiff must plead particular facts *existing at the times challenged statements were made* that are inconsistent with those statements. *See IBEW Local 595 Pension & Money Purchase Pension Plans v. ADT Corp.*, 660 Fed. Appx. 850, 857 (11th Cir. 2016).[4] Indeed, it is axiomatic that, to predicate a fraud claim on an alleged false statement, the statement must have been false at the time it was made by the speaker, not inferred to have been false in hindsight by virtue of after-the-fact events. *In re HomeBanc Corp. Sec. Litig.*, 706 F. Supp. 2d 1336, 1360 (N.D. Ga. 2010) ("Plaintiff's reliance upon after-the-fact events (*i.e.*, HomeBanc's ultimate demise) to support an inference that these and other earlier statements must have been intentionally misleading and made with scienter amounts to little more than fraud by hindsight, which is not actionable."); *Belmont Holdings Corp. v. SunTrust Banks, Inc.*, No. 1:09-CV-1185-WSD, 2010 WL 3545389, at *7 (N.D. Ga. Sept. 10, 2010) (finding that, in the context of alleged violations of Exchange

[4] In addition, under *Janus Capital Group, Inc. v. First Derivative Traders*, only the "maker" of a statement—"the person or entity with ultimate authority over the statement, including its content and whether and how to communicate it"—can be held liable under Rule 10b-5. 564 U.S. 135, 141-42 (2011). Mr. Smith is alleged to have made only Statements 7-11, 15-16, 21, 24-25, and 27-30; Mr. Gamble only Statements 7-11, 20, 24-25, and 27-30; Mr. Dodge only Statement 19; and Mr. Ploder only Statements 17-18. *See* Statement Chart. Under *Janus*, none of these Individual Defendants can face Section 10(b) liability for statements they are not alleged to have made. 564 U.S. at 141-42.

Act Sections 11 and 12, "[Plaintiff's] hindsight assessment does not permit the court to infer that SunTrust's financial assessments were false or misleading *at the time they were made*."); *In re Serologicals Sec. Litig.*, No. CIV. A. 1:00-CV-1025-CAP, 2003 WL 24033694, at *12 (N.D. Ga. Feb. 20, 2003) ("To avoid undermining the policies of the Reform Act, the court must refrain from relying on the magnitude of an overstatement, buttressed only by hindsight and speculation." (citations omitted)).

Plaintiff challenges the following categories of statements as purportedly false and misleading: (1) statements about Equifax's commitment to data security; (2) statements about the Company's data security standards and practices; (3) statements of opinion and belief about data security; (4) statements about cybersecurity risks; (5) statements about Equifax's internal controls; and (6) miscellaneous additional statements. As shown below, the Complaint fails to allege that any of these challenged statements were false or misleading when made, and the Complaint should be dismissed on this basis alone.

1. Statements About Equifax's Commitment to Data Security

Many of the challenged statements simply refer to or generally describe Equifax's commitment to and prioritization of data security. For example: "We have built our reputation on our commitment . . . to protect the privacy and

confidentiality of personal information about consumers. . . . Safeguarding the privacy and security of information, both online and offline is a top priority for Equifax." ¶ 286; Stmt. 1; *see also* ¶¶ 319, 334; Stmts. 13, 21. Additional statements of this type are set out in the Statement Chart under Tab A (hereinafter, the "Commitment Statements").[5] For the reasons explained below, Plaintiff fails to adequately plead that these statements were false or misleading.

a) Allegations of "inadequate" security measures are insufficient.

Plaintiff alleges that the Commitment Statements were misleading because "Equifax's cybersecurity and data protection measures were inadequate to secure the sensitive data in Equifax's custody" and Equifax purportedly "failed to implement basic data protection tools and procedures," including some allegedly recommended by consultants and so-called "security experts." *See* ¶¶ 287, 290, 299, 308, 317, 320, 322, 329, 331, 335, 337, 345. These allegations seek to dress up claims of corporate mismanagement as securities fraud and thus fail to state a Section 10(b) claim under well-settled law. Indeed, as the Supreme Court held forty years ago, "Congress by [enacting] § 10(b) did not seek to regulate [conduct]

[5] The Commitment Statements also include statements discussing Equifax's investments in data security, the care, effort, and resources devoted toward security, and the Company's goal to serve as a trusted steward of consumer data. *See* Statement Chart Tab A, Stmts. 2, 5, 7-8, 12, 14, 17-19, 22, 25.

which constitute[s] no more than internal corporate mismanagement." *Santa Fe*, 430 U.S. at 479-80. Allegations that Defendants should have implemented different or better security measures to protect data are, at most, allegations of "mismanagement," for which the securities laws do not provide a remedy. *See id*. Further, merely alleging a failure to disclose possible mismanagement and (even allegedly severe) operational problems does not state a Section 10(b) claim. *See Cutsforth v. Renschler*, 235 F. Supp. 2d 1216, 1242-44 (M.D. Fla. 2002) (applying *Santa Fe* and dismissing claims similarly based on alleged failure to disclose "severe problems" with computer systems and other operational problems following a merger); *accord Craftmatic Sec. Litig. v. Kraftsow*, 890 F.2d 628, 640 (3d Cir. 1989); *In re Winn-Dixie Stores, Inc. Sec. Litig.*, 531 F. Supp. 2d 1334, 1347 (M.D. Fla. 2007); *In re Donna Karan Int'l Sec. Litig.*, 1998 WL 637547, at *9 (E.D.N.Y. Aug. 14, 1998).

At least one federal court has rejected substantively identical securities fraud claims predicated on allegations that the failure to implement adequate cybersecurity measures and adopt recommended reforms resulted in a significant cybersecurity incident, and this Court should do the same. Specifically, in *Heartland*, the plaintiffs alleged that the defendants misrepresented the general state of data security at Heartland, a payment processing company, prior to a cyber

attack that resulted in the theft of 130 million credit and debit card numbers, contending that the breach proved that those statements had been false or misleading. 2009 WL 4798148 at *4-6. The court dismissed the plaintiff's claims, however, holding that "[t]he fact that a company has suffered a security breach does not demonstrate that the company did not 'place significant emphasis on maintaining a high level of security.'" *Id.* at *5. Specifically, the court held that the breach did not render the defendants' aspirational statements about security false or misleading, finding that it was more plausible that "Heartland did place a high emphasis on security but that the Company's security systems were nonetheless overcome." *Id.* (opining further that "the alleged facts are more plausibly explained by lawful behavior than illegal deception").

The *Heartland* court also rejected allegations that "unresolved security issues remaining in the wake of [an earlier, and undisclosed, cyber attack]" made statements generally describing the company's data security practices false or misleading. *Id.* at *5-6. This included, for example, the allegation that a "former Senior Developer at Heartland" complained of inadequate security practices and criticized the company for failing to do more to contain the breach and improve security. *Id.* at 5. The court found these allegations insufficient, opining that,

among other things, "the fact that a company faces certain security problems does not of itself suggest that the company does not value data security." *Id*.

Plaintiff's allegations in this case are virtually identical, and they, too, should be dismissed. *Compare, e.g., Heartland*, 2009 WL 4798148 at *5-6 (addressing statements that Heartland "place[d] significant emphasis on maintaining a high level of security" and maintained a network configuration that "provides multiple layers of security to isolate our databases from unauthorized access"), *with, e.g.*, Statement Chart Tab A Stmts. 1 ("Safeguarding the privacy and security of information, both online and offline, is a top priority for Equifax."); 13 (noting Equifax's "unwavering commitment to security"); 8 ("We continue to invest in and develop new technology to enhance the functionality, cost-effectiveness and security of the services we offer"); 19 ("data security and how we go about ensuring that is something we spend a lot of time and effort on").

Simply stated, the fact that a company has become the victim of a significant cyber attack does not render false the company's prior statements about its commitment to data security or its efforts to secure its data, nor do allegations that it faced certain security challenges before the attack or declined to adopt some security recommendations alleged to have been made by consultants, purported "experts," or others. ¶¶ 69-94. *See Heartland*, 2009 WL 4798148 at *5-6.

b) Defendants did not mislead investors by "failing" to disclose the Cybersecurity Incident earlier.

Plaintiff also alleges that certain of the Commitment Statements (Stmts. 1, 5, 12, 21, & 22) were misleading by omission because Defendants did not publicly disclose the Cybersecurity Incident earlier than September 7, 2017. ¶ 318, *see also* ¶¶ 288, 300, 335, 338. However, Section 10(b) does not impose fraud liability based solely on incomplete statements. Nor is the mere non-disclosure of material information actionable in a private lawsuit. *See, e.g.*, *Heartland*, 2009 WL 4798148, at *6 ("If Plaintiffs had known of the SQL attack, they might not have purchased Heartland securities. However, there is no general duty on the part of issuers to disclose every material fact to investors."). Instead, under Section 10(b) and Rule 10b-5, "[d]isclosure is required . . . only when necessary 'to make . . . statements made, in the light of the circumstances under which they were made, not misleading.'" *Matrixx Initiatives, Inc. v. Siracusano*, 562 U.S. 27, 44 (2011) (quoting Rule 10b-5(b)). Plaintiff's omission allegations do not satisfy this standard and thus fail to state a claim.

First, Plaintiff cannot show that any Commitment Statements alleged to have been made *prior to* Equifax's alleged discovery of suspicious activity on its Dispute Portal in late July 2017 were false. As a matter of common sense, no Defendant could have intentionally misled anyone as to facts about which he had

no knowledge. *See In re Discovery Labs. Sec. Litig.*, 2006 WL 3227767, at *9 (E.D. Pa. Nov. 1, 2006) ("plaintiffs must, at a minimum, allege the existence of some fact, known to defendants at the time of the statements" which made the statements false or misleading). Here, Plaintiff's own allegations confirm that ***no one at Equifax had discovered the suspicious activity until July 29, 2017 at the earliest***. ¶ 116. This allegation alone precludes any claim that statements made in May and June 2017 (or earlier) referencing Equifax's "investments to address critical data security" and "role as a trusted steward" (¶¶ 316, 318; Stmt. 12) were misleading based on the "failure" to disclose a security breach that no one at Equifax is alleged to have known *anything* about until months later. *See In re Discovery Labs.*, 2006 WL 3227767, at *9.

Second, the fact that a company has experienced a cybersecurity incident does not render aspirational statements about that company's data security efforts misleading. In *Heartland*, for example, the court rejected plaintiffs' attempt to rely on the non-disclosure of an earlier cyber attack as the basis for Section 10(b) claims despite management's discovery of the attack in late 2007, and public statements during 2008 regarding the Company's emphasis on cybersecurity. *See Heartland*, 2009 WL 4798148, at *6. Rather, the court held that "the fact that a company faces certain security problems does not of itself suggest that the

company does not value data security." *Id*. at *5. The court held further that where, like the Commitment Statements challenged here, Heartland's statements did not say "the company's network was immune from security breaches or that no security breach had ever occurred," those statements were not made misleading by an alleged failure to disclose the earlier attack. *Id.* at 6.

For all of the above reasons, Plaintiff fails to state any claim based on the alleged "failure" to disclose the Cybersecurity Incident between July 29 and September 7, 2017.

c) Vague and generalized statements reflecting optimism and aspiration are not actionable in any event.

Plaintiff's claims challenging the Commitment Statements also fail for the additional and independent reason that these generalized, non-verifiable, and vague statements of commitment to and aspirations about data security "are not actionable because reasonable investors do not rely on [such statements] in making investment decisions." *Amalgamated Bank v. Coca-Cola*, No. 1:05-CV-01226-RWS, 2006 WL 2818973, at *3 (N.D. Ga. Sept. 29, 2006) (holding that "such statements of 'corporate optimism' or 'puffery,' in addition to lacking [an] underlying factual basis, also fail the materiality requirement of Rule 10b-5"), *aff'd sub nom. Selbst v. Coca-Cola Co.*, 262 F. App'x 177 (11th Cir. 2008). As a matter of law, no Section 10(b) claim can be predicated on such statements. *Id*.

Many of the Commitment statements, which generally avow a commitment to data security or characterize security as a priority for Equifax, fall into this category of non-actionable statements. *See* Stmts. 1 (discussing "commitment . . . to protect the privacy and confidentiality of personal information" and stating that "[s]afeguarding the privacy and security of information, both online and offline, is a top priority for Equifax."); 13 (claiming "unwavering commitment" to security); 21 (data security "is a huge priority"). Courts repeatedly have held that no reasonable investor would rely on such vague and generalized statements. *See, Chipotle II*, 294 F. Supp. 3d at 232 (similar statements of commitment to food safety were non-actionable "puffery"); *In re Australia & New Zealand Banking Grp. Ltd. Sec. Litig.*, 2009 WL 4823923, at *11 (S.D.N.Y. Dec. 14, 2009) (dismissing claims challenging statements that "[m]anagement is committed to achieving a strong risk control" and "committed to best practice in preparing its financial statements"); *Heartland*, 2009 WL 4798148, at *5 (statement that company "place[d] significant emphasis on maintaining a high level of security" was not actionable despite breach, especially because company never claimed that it was "invulnerable" to attack).

Other Commitment Statements refer generally and without specifics to investments in and time spent on data security and efforts to comply with data

security laws and regulations. *See* Stmts. 8 ("We continue to invest in and develop new technology to enhance the . . . security of the services we offer.") and 9, 12, & 19 (similar); *see also* Stmts. 25 (Equifax "devot[es] substantial compliance, legal and operational business resources to facilitate compliance with applicable regulations and requirements") and 22 (similar). Courts have found analogous statements of investment in and devotion of resources to compliance efforts and related corporate goals are not actionable. *See In re Ocwen Financial Corp. Sec. Litig.*, 2015 WL 12780960, at *15 (S.D. Fla. Sept. 4, 2015) (dismissing claims challenging general statements about "investments in risk and compliance"); *Perez v. Higher One Holdings, Inc.*, 2016 WL 6997160, at *13 (D. Conn. Sep. 13, 2016) (statements about "improvements and investments in compliance" not actionable).[6]

The remaining Commitment Statements reference Equifax's goal to serve as a "trusted steward" of data. *See* Stmts. 7, 13, 15, 18-19. These generalized,

[6] Challenged statements describing *efforts* to "ensure" or "facilitate" data security and compliance with regulations, laws, standards, or "best practices" were not stated as guarantees of perfect security or compliance. ¶¶ 298, 336; 344; Stmts. 5, 22, 25; *see also* ¶¶; 292, 339, 342, 346; Stmts. 3, 23-24, 26. As such, Plaintiff's conclusory allegations that Equifax's practices purportedly fell short of satisfying certain regulations, laws, standards, or best practices (¶¶ 293, 337, 340, 343, 345, 347)—even were they supported by competent factual allegations (and they are not)—fail to establish actionable misrepresentations. *See Chipotle II*, 294 F. Supp. 3d at 232-33 (statements about food safety efforts did not amount to guarantees of the efficacy of those efforts and thus were not actionable).

aspirational statements are non-actionable as well. *See, e.g.*, *Chipotle II*, 294 F. Supp. 3d at 232-33; *Martin v. GNC Holdings, Inc.*, 2017 WL 3974002, at 8 (W.D. Pa. Sept. 8, 2017) (statements that company was an "industry leader" and "set[] the [industry] standard" were not actionable).

2. Statements About Data Security Standards and Practices

Plaintiff's claims based on several alleged statements about Equifax's data security standards and data security compliance practices likewise fail for several reasons. *E.g.*, ¶ 289 ("Equifax employs strong data security and confidentiality standards"); ¶ 339 ("Equifax uses a variety of technical, administrative and physical ways to keep personal credit data safe."); ¶ 342 ("We continuously monitor federal and state legislative and regulatory activities . . . in order to remain in compliance with all applicable laws and regulations."); *see also* ¶¶ 292, 295, 298, 301, 311, 339, 342, 346; Stmts. 2-4, 6, 11, 23-24, 26 (the "Standards and Practices Statements"); *see also* Statement Chart Tab B.

First, these allegations merely allege purported internal mismanagement, or the failure to disclose such mismanagement, which does not constitute securities fraud. *See* ¶¶ 290, 293, 296, 299, 302, 312, 340, 347. Rather, as discussed more fully in § III.A.1.a., such allegations fail to state a Section 10(b) claim.

Second, these allegations cannot survive dismissal because they fail to plead the falsity of each of the Standards and Practices Statements with particularity. For example, Plaintiff challenges a statement published on Equifax's website that "[t]he Equifax network is reviewed on a continual basis by external security experts who conduct intrusion testing, vulnerability assessments, on-site inspections, and policy/incident management reviews." ¶ 292; Stmt. 3. Plaintiff alleges that this statement was misleading because Equifax's cybersecurity reviews were not "adequate" and because the Company declined to implement some "advice" from such experts (and others). But these allegations do not contradict the statement that the network was reviewed and that testing, assessment, inspections, and reviews were performed—they merely second-guess the extent or efficacy of such efforts. *Id.* Plaintiff similarly fails to plead facts contradicting statements that Equifax had an enterprise risk management program targeting controls relating to, among other things, data security (¶ 346; Stmt. 26);[7] "used a variety of technical, administrative and physical ways to keep personal credit data safe" (¶ 339; Stmt. 23); "regularly review[ed] and update[d] [its] security protocols" (*id.*); "monitor[ed] federal and state legislative and regulatory activities

[7] The allegation that Equifax announced efforts to strengthen its enterprise risk management program after the Class Period (¶ 347) does not show that statements about the program allegedly made one year earlier were false when made.

that involve credit reporting, data privacy and security" (¶ 342; Stmt. 24); and "develop[ed], maintain[ed], and enhance[ed] secured proprietary information databases" (¶ 311; Stmt. 11). Absent credible allegations that Equifax did not in fact have an enterprise risk management program, or allegations that Equifax did not attempt to comply with relevant data security rules and regulations, allegations of the inadequacy or failure of such efforts do not support a securities fraud claim.

Chipotle II is instructive. There, the plaintiffs challenged various statements positively describing Chipotle's existing food safety standards, programs, and procedures. *See Chipotle II,* 294 F. Supp. 3d at 232. As here, the plaintiffs in *Chipotle II* did not allege that the company had no such standards, programs, and procedures in place. *Id.* Instead, the plaintiffs relied on allegations that those measures were "inadequate," "inherently deficient," or poorly executed. *Id.* The court held that these allegations, which did not "conflict with Defendants' statements regarding the . . . programs and procedures that Chipotle had in place, but merely quibble[d] with [the] execution of those programs and procedures," failed to adequately plead the statements' falsity. *Id.* The same shortcoming dooms Plaintiff's attack on the Standards and Practices Statements.[8]

[8] Plaintiff also alleges that certain of the Standards and Practices Statements were false and misleading because they remained on Equifax's website in the interval

Third, as with the Commitment Statements, many of the Standards and Practices Statements are "puffery"—vague, generalized statements of corporate optimism upon which no reasonable investor would rely. *See* Stmts. 2 (referencing "strong data security and confidentiality standards" and "highly sophisticated data information network"); 6 (referring to "award-winning technology" and "proven track record of handling sensitive data"); 23 (aspiration to "continue to meet or exceed established best practices at all times"); 24 (discussing efforts to "remain in compliance with all applicable laws and regulations"); 26 ("We have a rigorous enterprise risk management program"); *see also Chipotle II*, 294 F. Supp. 3d at 232-33 (observing that similar generalized statements of corporate optimism and compliance efforts were non-actionable "puffery"); *see also* Section III.A.1.c.[9]

3. Statements of Opinion and Belief

Plaintiff also challenges various statements expressing opinions and beliefs about data security-related topics, such as Mr. Smith's May 18, 2016 statement expressing the opinion that "I think we are in a very good position [as to data

---

between Equifax's alleged discovery of unauthorized access of its network on July 29, 2017 and its announcement of the Cybersecurity Incident on September 7, 2017. ¶¶ 291, 294, 297, 303, 341, 348; Stmts. 2-4, 6, 23, 26. These allegations fail to state a claim for the reasons discussed in Section III.A.1.b.

[9] As held in *Heartland*, the occurrence of a significant cybersecurity attack does not indicate that a company lacked commitment to security or failed to undertake serious efforts to protect against such attacks. 2009 WL 4798148 at *5-6.

security] now . . . feel like we're in really good shape." ¶ 323; Stmt. 15. To adequately plead the falsity of such subjective statements of opinion or belief, a plaintiff must allege facts establishing that the speaker did not, in fact, hold the stated opinion or belief.[10] *See City of Omaha, Nebraska Civilian Employees' Ret. Sys. v. CBS Corp.*, 679 F.3d 64, 67 (2d Cir. 2012); *accord Va. Bankshares, Inc. v. Sandberg*, 501 U.S. 1083, 1095 (1991); *City of Edinburgh Council v. Pfizer, Inc.*, 754 F.3d 159, 170 (3d Cir. 2014); *Nolte v. Capital One Fin. Corp.*, 390 F.3d 311, 315 (4th Cir. 2004). Plaintiff has not satisfied this standard. Putting aside the fact

[10] In *Omnicare, Inc. v. Laborers District Council Construction Industry Pension Fund*, the U.S. Supreme court held that opinion statements may be misleading *for purposes of claims under Section 11 of the Securities Act of 1933* if (1) the speaker did not in fact hold the belief expressed; (2) some fact stated as support for the opinion was untrue; or (3) the omission of "particular (and material) facts . . . about the inquiry the issuer did or did not conduct or the knowledge it did or did not have" made the statement misleading. 135 S. Ct. 1318, 1327, 1332 (2015). Courts have expressed reluctance to extend *Omnicare* to claims under the Exchange Act, which have different and more exacting elements than Section 11 claims. *See, e.g.*, *Firefighters Pension & Relief Fund of the City of New Orleans v. Bulmahn*, 147 F. Supp. 3d 493, 527–28 (E.D. La. 2015), *aff'd sub nom. Neiman v. Bulmahn*, 854 F.3d 741 (5th Cir. 2017) ("It is not clear, however, that the Supreme Court's analysis in *Omnicare* extends to securities fraud claims under Section 10(b) of the Securities Act of 1934. Section 11 of the 1933 Act and Section 10(b) of the 1934 differ in significant ways."); *Hoey v. Insmed Inc.*, 2018 WL 902266, at *16 & n.14 (D.N.J. Feb. 15, 2018) (noting absence of guidance on application of *Omnicare* to Section 10(b) claims and joining other courts in applying pre-*Omnicare* standard requiring a showing that opinion statements are "not honestly believed and lack a reasonable basis" to be actionable). In any event, even if the *Omnicare* standards apply here, Plaintiff has not satisfied them.

that this statement is alleged to have been made more than one year before anyone at Equifax is alleged to have learned of the attack, and more than nine months before the Apache Struts vulnerability was even discovered, there is no allegation that Mr. Smith did not, in fact, believe that Equifax was in "good shape" regarding data security when making this statement in May 2016. ¶ 324. Instead, Plaintiff merely repeats its allegation that Equifax's cybersecurity measures were "inadequate," which is insufficient to plead falsity under *Santa Fe* (*see* Section III.A.1.a.). ¶ 324.[11]

4. Statements About Cybersecurity Risks

Plaintiff attempts to avoid the reality that Equifax expressly and repeatedly warned about the potential for criminal security breaches by contending that those very warnings, included in the Company's Forms 10-K—"our information technology networks and infrastructure . . . could be vulnerable to . . . breaches of confidential information due to criminal conduct . . . or other advanced persistent

[11] Challenged statements opining as to the strength or security of Equifax's data protection measures (Stmts. 2, 4, 6, 11, 20, 26) and the extensiveness of Equifax's security and compliance efforts (Stmts. 5, 8, 9, 19, 22-25), characterizing the Company as a trusted steward of data (Stmts. 2, 7, 12-14, 17-18), and stating that the Company was not aware of a material data breach prior to discovery of the Cybersecurity Incident (Stmt. 10) likewise convey opinions and beliefs on those subjects that Plaintiff has not adequately pled the speakers did not hold. *See* Statements Chart Tab C. Claims challenging these statements must be dismissed for this reason as well as others explained herein.

attacks by hackers"—were themselves somehow false. ¶ 306; Stmt. 9; *see also* Statement Chart Tab D (cybersecurity risks statements). Under Plaintiff's misguided theory, these warnings were misleading because Equifax should have said that it "was" vulnerable to attack rather than that it "could" be vulnerable. ¶ 308.

These allegations fail to state a fraud claim. *See Heartland*, 2009 WL 4798148 at *5-6 (rejecting challenge to similar disclosures about risks of cyber attacks). Indeed, where, as here, an issuer repeatedly warns of the precise risk to which a plaintiff attributes its losses,[12] the issuer has made "the appropriate disclosures" and "cannot be held liable for failure to disclose." *Zagami v. Cellceutix Corp*., 2016 WL 3199531, at *14 (S.D.N.Y. June 8, 2016); *accord Ong v. Chipotle Mexican Grill, Inc. ("Chipotle I")*, 2017 WL 933108, at *11 (S.D.N.Y. Mar. 8, 2017); *see also In re Leapfrog Enters., Inc. Sec. Litig.*, 527 F. Supp. 2d. 1033, 1048-49 (N.D. Cal. 2007) (rejecting claim that defendants should have said adverse factors "are" affecting financial results rather than "may" affect financial results); *Harris v. Ivax Corp.*, 182 F.3d 799, 807 (11th Cir. 1999) (where disclosures "warned of risks of a significance similar to that actually realized,

[12] In addition to the risk factors in Equifax's SEC filings, Plaintiff alleges that Mr. Smith warned at a May 2016 investor conference that "a lot of people with a lot of time on their hands [are] trying to crack [Equifax's databases]." ¶ 323; Stmt. 15.

[investors were] sufficiently on notice"). Far from constituting securities fraud, these disclosures show that Equifax and its management warned shareholders about the very risk that eventually occurred, prompting this lawsuit.

Plaintiff's allegation that Equifax also failed to disclose material information required to be disclosed by Item 303 of Regulation S-K—specifically that Equifax's "data protection measures were inadequate to secure the sensitive data in Equifax's custody, and that additional changes to its cybersecurity were needed to prevent a significant data breach"—likewise fails to state claim for relief. ¶¶ 313-14. *First*, there is no private right action under Section 10(b) for an alleged violation of Item 303. *See Ash v. PowerSecure Int'l, Inc.*, 2015 WL 5444741, at *11 (E.D.N.C. Sept. 15, 2015).[13] *Second*, to the extent that a Section 10(b) claim may be predicated on an alleged non-disclosure under Item 303, Plaintiff has not pled an Item 303 violation.

Item 303 addresses only the obligation to disclose *known* trends and uncertainties. *See In re Bank of Am. AIG Disclosure Sec. Litig.*, 980 F. Supp. 2d

[13] Although the Second Circuit has held an alleged failure to disclose information pursuant to Item 303 can serve as the basis for a securities fraud claim under Section 10(b), the Ninth and Third Circuits have reached the opposite conclusion. *Compare Stratte-McClure v. Morgan Stanley*, 776 F.3d 94, 100 (2d Cir. 2015); *with In re NVIDIA Corp. Sec. Litig.*, 768 F.3d 1046, 1054-56 (9th Cir. 2014); *Oran v. Stafford*, 226 F.3d 275, 288 (3d Cir. 2000). Neither the Eleventh Circuit nor the U.S. Supreme Court has issued a ruling on this question that would bind this Court.

564, 584 (S.D.N.Y. 2013) (discussing Item 303's requirement that a trend or uncertainty be "presently known," not merely "reasonably possible"). But Plaintiff pleads no facts establishing that Defendants knew Equifax's "data protection measures were inadequate to secure the sensitive data in Equifax's custody" or that a significant data breach was likely to occur.[14] Plaintiff's Item 303 allegations thus fail to state a claim. *Id.*; *see also Chipotle I*, 2017 WL 933108, at *11 ("Corporate officials need not be clairvoyant"); *id*. at *17 ("Item 303 requires the disclosure of harm that is probable, imminent, and not merely potential."). Equifax satisfied Item 303 by disclosing the risk of breach of its networks and infrastructure housing confidential information "due to criminal conduct . . . or other advanced persistent attacks by hackers." ¶ 306; *see Chipotle I*, 2017 WL 933108, at *11 (disclosures that warned of the risks of events that later occurred satisfied Item 303).

Finally, Plaintiff fails to adequately allege that it was misleading for Equifax to incorporate by reference in Forms 10-Q filed on April 27, 2017 and July 27, 2017 a statement from prior Forms 10-K that the Company was "not aware of any material breach of our data, properties, networks, or systems," given that "hackers had already penetrated Equifax's internal data systems and accessed sensitive

[14] Alleged failure to disclose the purported "inadequacy" of Equifax's data protection measures or that Defendants mismanaged cybersecurity, is also insufficient to state a claim under *Santa Fe*. *See* Section III.A.1.a.

personal information." ¶¶ 309-10. This is because, as Plaintiff concedes, Equifax first discovered the suspicious activity on its Dispute Portal on July 29, 2017, ***after*** both challenged 10-Qs had already been filed. ¶ 116. As such, these allegations fail to state a claim. *See Discovery Labs.*, 2006 WL 3227767, at *9 ("plaintiffs must, at a minimum, allege the existence of some fact, known to defendants at the time of the statements").

5. Statements About Internal Controls

Plaintiff also challenges statements in Equifax's Forms 10-K discussing "management's" (including Defendants Smith and Gamble) review of and conclusions regarding Equifax's internal controls over financial reporting and the Company's disclosure controls. *See* ¶ 349 (Stmt. 27); Ex. D at 98; Ex. E at 97 (stating that "management concluded that . . . Equifax's internal control over financial reporting was effective" and that such controls included controls intended to "provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of our assets that could have a material effect on the financial statements"); ¶ 350 (Stmt. 28); Ex. D at Exhibit 31.1 & 31.2; Ex. E at Exhibit 31.1 & 31.2 (based on Mr. Smith's and Mr. Gamble's evaluation of financial reporting controls, "significant deficiencies and material weaknesses in the design or operation of" financial reporting controls

were disclosed to Equifax's auditors and the audit committee of its board); ¶¶ 350-51 (Stmts. 29-30); Ex. D at 98; Ex. E at 97 (statements of Mr. Smith's and Mr. Gamble's conclusions that Equifax's disclosure controls were "designed to provide reasonable assurance of achieving their objectives" and "provided reasonable assurance" that information required to be publicly reported was communicated to management to allow for timely decisions regarding disclosure). *See* Statements Chart E (internal controls statements).

Plaintiff alleges that these statements were misleading because "Equifax lacked adequate internal mechanisms for detecting breaches of its data networks and failed to design and implement an adequate data breach protocol that would facilitate prompt and materially complete disclosure of such breaches." ¶ 352. But this allegation fails to plead the falsity of challenged statements which addressed Equifax's internal controls over *financial reporting* (as opposed to controls over data security, "breach protocol," or disclosure). *See In re Banco Bradesco S.A. Sec. Litig.*, 277 F. Supp. 3d 600, 648-49 (S.D.N.Y. 2017) (dismissing claims challenging certifications about financial reporting controls where plaintiff failed to allege any failure in financial reporting (*e.g.*, a need to restate published financial results)) (citing cases). Plaintiff fails, for this reason alone, to plead the falsity of Statements 27-28, which exclusively addressed financial reporting

controls. *Id.*; *see also In re PetroChina Co. Ltd. Sec. Litig.*, 120 F. Supp. 3d 340, 359-60 (S.D.N.Y. 2015) (allegations that defendant lacked controls sufficient to prevent alleged bribery offenses did not plead falsity of statements about financial reporting controls).

Further, Plaintiff cannot adequately plead the falsity of statements pertaining to disclosure controls (Statements 29-30) simply by alleging the failure to detect and disclose the Cybersecurity Incident earlier. *See Banco Bradesco*, 277 F. Supp. 3d at 648 (rejecting similar hindsight allegations based on alleged controls failures) (citing cases). As in *Banco Bradesco*, the disclosure controls statements challenged here "do not purport to guarantee that [the] controls will perform perfectly in every instance; instead, they speak to "*reasonable* assurance." 277 F. Supp. 3d at 648 (emphasis added). Where, as in *Banco Bradesco*, Plaintiff has not pled that "management did not, in fact, conduct the evaluations described in those statements, that its internal controls were not 'designed' to provide reasonable assurance [of achieving their objectives], that the Company did not have internal controls or did not execute them, or that the Company had identified but not disclosed significant deficiencies or material weaknesses," Plaintiff has failed to state a claim. *Id.*

6. Other Challenged Statements

Plaintiff also fails to adequately plead the falsity of the remaining challenged statements, both of which concern matters unrelated to the Cybersecurity Incident on which Plaintiff's claims are based. *See* Statements Chart F (other challenged statements).

In one such statement, Mr. Gamble described an income exchange offered by the Workforce Solutions business segment that enables third parties needing to verify a person's income and employment status (*e.g.*, prospective lenders) to do so without requiring the employers independently to confirm the *bona fides* of the party seeking the verification. ¶ 332; Stmt. 20. Among other things, Mr. Gamble is alleged to have said that the "income exchange . . . provides a secure verification network" and that "we make sure that the people accessing that information [on the exchange] have a right to see it." *Id.* Plaintiff fails, however, to plead any facts demonstrating that these statements were untrue or misleading when made. Plaintiff does not allege, for example, that the income exchange to which the statement referred was known or ever revealed to have been *un*secure when Mr. Gamble made the statement. Instead, Plaintiff relies on conclusory and unsupported allegations of unspecified data security "inadequa[cies]" elsewhere

within Equifax's organization. ¶ 333. The allegations fail to plead the falsity of Mr. Gamble's statement.

Plaintiff also fails to plead the falsity of statements about the so-called "W2Express Breach," wherein Defendant Smith discussed implications of an Equifax client's decision to enable the client's employees to access W-2 information using a "simple passcode" rather than a more complicated passcode. ¶ 325; Stmt. 16. Indeed, Plaintiff alleges that the "W2Express Breach" was facilitated by use of a "four-digit pin code" authentication protection, ¶ 73, which does not contradict and is instead consistent with the challenged statement about that incident involving W2Express. Although Plaintiff also alleges that an unidentified source purportedly claimed that the four-digit pin code authentication was "the standard Equifax setup," *id.*, Plaintiff does not plead any facts contradicting the statement that Equifax urged the client to use "a more complicated passcode," which Equifax claimed to have done. ¶ 325.

B. Plaintiff Fails To Plead A Strong Inference Of Scienter.

To meet the exacting standards of the PSLRA for pleading that Defendants made the alleged misstatements with scienter, Plaintiff must allege that the speaker acted with wrongful intent, such as an intent to deceive—and not merely that certain statements were inaccurate or mistaken. Further, Plaintiff must plead facts

that give rise to an inference of scienter that is "cogent," "strong," and "at least compelling as any opposing [non-fraudulent] inference one could draw from the facts alleged." *Tellabs*, 551 U.S. at 324. *See also Mizzaro*, 544 F.3d at 1238 (plaintiff must plead facts raising a "strong" and "compelling" inference of wrongful intent). Plaintiff also must plead facts supporting a strong inference of scienter "for ***each*** defendant with respect to ***each*** violation." *Phillips v. Scientific-Atlanta, Inc.*, 374 F.3d 1015, 1016 (11th Cir. 2004). Plaintiff fails to satisfy these standards and thus fails to plead scienter as to any Defendant.

Plaintiff's scienter allegations fall into five categories: (1) alleged prior warnings of inadequate data security that preceded the Cybersecurity Incident; (2) allegations derived from mischaracterization of Mr. Smith's post-Incident testimony; (3) allegations concerning knowledge of the Cybersecurity Incident itself; (4) additional allegations of scienter; and (5) allegations about stock sales by two defendants.

1. Alleged Warnings About Data Security Fail to Plead Scienter.

Plaintiff's allegations about purported "warnings . . . that Equifax's cybersecurity was inadequate" (¶¶ 268-271) fail to raise the required strong inference of scienter as to any Individual Defendant. Plaintiff fails to plead facts establishing that any of the alleged "warnings" purportedly conveyed by "security

researchers," Equifax employees, or Deloitte were ever communicated to any Individual Defendant. ¶¶ 3, 12-13, 72, 77-83, 94, 202, 209, 213, 218, 235, 243, 246, 254, 269, 271. These allegations fail for this reason alone. *See Fidel v. Rampell*, 2005 WL 5587454, at *4, *7 (S.D. Fla. Mar. 29, 2005) (declining to infer scienter when complaint failed to allege that defendants were directly told specific information that contradicted their public disclosures); *Mogensen v. Body Cent. Corp.*, 15 F. Supp. 3d 1191, 1220 (M.D. Fla. 2014) (adequately pleading scienter requires "specific details of first-hand interactions with a defendant in which they advised him that existing facts contradicted his public disclosures").

Plaintiff further alleges—based only on third-party articles from *Bloomberg* and *Motherboard*—that Equifax's patching process had unspecified issues or was otherwise deficient. ¶¶ 91-93, 78; *see also* ¶¶ 13, 110, 268. Plaintiff cites the *Bloomberg* article to allege that Equifax engaged Mandiant to conduct a cybersecurity audit that reported certain unspecified findings regarding patching in March 2017. ¶¶ 91-93; *see also* ¶¶ 13, 110, 268. Only two of the *Bloomberg*-based allegations could bear on *any* Individual Defendant's scienter—(i) that Mr. Smith "was personally overseeing" Mandiant's work, and (ii) that at some unspecified time, "Mandiant warned Equifax that its unpatched systems and misconfigured security policies could indicate major problems." ¶¶ 91-92. But

both of these are attributed solely to anonymous sources. ¶ 91 ("Smith was overseeing [Mandiant's work] personally, *according to one person with direct knowledge of the matter*"); ¶ 92 ("Bloomberg reported, 'Mandiant warned Equifax that its unpatched systems and misconfigured security policies could indicate major problems, *a person familiar with the perspectives of both sides said*.'"). Plaintiff's allegation that Equifax's "systems patching process was deficient," ¶ 78, similarly relies on an article from *Motherboard*, which likewise relies on anonymous sources unconnected in time and place to the Cybersecurity Incident. Under the federal securities laws, these anonymous sources carry no weight because they fail to specify *any* bases for the sources' information, much less "unambiguously provide in a cognizable and detailed way the basis of the [source's] knowledge." *Mizzaro*, 544 F.3d at 1239-40 (suggesting that the weight given anonymous sources could be "eviscerate[d]" by a plaintiff's failure to "fully describe[] the foundation or basis of the confidential witness's knowledge, including the position(s) held, the proximity to the offending conduct, and the relevant time frame").

Even if Plaintiff had adequately pled the bases of the anonymous sources' knowledge for these assertions, however, the allegations still would not raise a strong inference of scienter. Plaintiff does not allege that Defendants Gamble,

Ploder, or Dodge were contemporaneously aware of any alleged Mandiant audit—which Plaintiff alleges was a "top-secret project"—much less that any ensuing findings were communicated to these Defendants during the Class Period. ¶¶ 13, 268; *see also* ¶¶ 91-93, 110. And critically, Plaintiff fails to allege precisely *when* (if at all) Mandiant communicated to Mr. Smith any concerns about patching issues or other aspects of Equifax's security. On this basis alone, the allegations fail to raise a strong inference that any Individual Defendant knew that any of his statements were misleading or acted with severe recklessness, and therefore fail to adequately plead scienter. *See Mizzaro*, 544 F.3d at 1238 (a plaintiff must plead with particularity facts giving rise to a strong inference that defendants acted with scienter when they made the challenged statements).

Further, Plaintiff fails to plead facts establishing that the Individual Defendants shared any concerns alleged to have been articulated by Mandiant (or were severely reckless in failing to do so in light of all pertinent and available information). *See, e.g.*, *Heartland*, 2009 WL 4798148, at *7-8 (finding scienter not adequately pled where allegations failed to show defendants believed data security measures were deficient); *In re HomeBanc*, 706 F. Supp. 2d 1336, 1350 (N.D. Ga. 2010) (dismissing complaint where plaintiff failed to establish that defendants agreed with others' assessments of "massive and systematic

problems"); *see also In re Royal Caribbean Cruises, Ltd. Sec. Litig.*, 2013 WL 3295951, at *18 (S.D. Fla. Apr. 19, 2013) (similar). Notably, Plaintiff omits mentioning that the same unsourced *Bloomberg* article on which it stakes much of its claims also reports Equifax's assessment that "Mandiant had sent an undertrained team without the expertise it expected from a marquee security company." *See* Ex. F. The article itself therefore suggests that Equifax was skeptical of Mandiant's alleged concerns, which would be a more plausible (and non-fraudulent) explanation than the inference Plaintiff urges, *i.e.*, that Equifax acted with severe recklessness by refusing to address a known, substantial and imminent threat to its data security. *Tellabs*, 551 U.S. at 328-29 (courts must weigh inferences against scienter that reasonably arise from plaintiffs' allegations).

Plaintiff's remaining allegations that certain alleged "warnings" put Defendants on notice that Equifax's security was "inadequate" likewise fail to raise a strong inference of scienter. Although Plaintiff references earlier alleged incidents involving W2Express and TALX, Plaintiff pleads no facts whatsoever to support its conclusory assertion that Defendants purportedly "knew that [these incidents] were symptomatic of fundamental institutional data security failures and

that those failures remained unremediated."[15] ¶ 270. Indeed, Plaintiff does not—and cannot—allege that Equifax had ever previously experienced an incident of the type disclosed on September 7, where criminal actors penetrated its systems by exploiting a software vulnerability and then ex-filtrated large amounts of data. Rather, Plaintiff relies upon unrelated prior incidents not alleged to have involved either intrusion of Equifax's internal systems or large-scale exfiltration of personal data. Therefore, notwithstanding Plaintiff's wholly conclusory effort to conflate these unrelated prior incidents with the Cybersecurity Incident, there was no meaningful overlap, and those prior incidents were not any sort of "red flag" warning of the circumstances that eventually gave rise to the Cybersecurity Incident.

Plaintiff also fails to allege particular facts showing that Defendants (i) knowingly disregarded warnings about the Apache Struts vulnerability that cybercriminals exploited in the Cybersecurity Incident or (ii) knew that Equifax had not applied the patch or that the Company's subsequent scans did not detect

[15] Plaintiff does not and cannot explain how these incidents (which impacted just two discrete services offered by the Workforce Solutions business segment and allegedly arose because cybercriminals were able to crack individual employees' passcodes on web portals maintained for their employers) contradicted any of Defendants' statements or could have alerted Defendants that Equifax's "internal systems" (¶ 270) were vulnerable to an attack like the Cybersecurity Incident, involving data exfiltration.

the continued vulnerability. ¶ 271. But even if Plaintiff could plead facts sufficient to support such allegations (and Plaintiff has not), such allegations would, at best, allege arguable mismanagement—not an intent to defraud investors *see* Section III.A.1.a.—and thus could not give rise to a strong inference of scienter. *See Mogensen*, 15 F. Supp. 3d at 1218 ("Even reasonable and plausible fraud cases will be dismissed if an inference of poor business judgment—and even negligence or mismanagement—flows even slightly more naturally from the well-pled factual allegations than does an inference of scienter.").

2. Allegations Concerning Mr. Smith's Testimony Do Not Support Scienter.

Plaintiff also attempts to allege scienter through allegations about portions of Mr. Smith's post-Class Period testimony before various Congressional Committees that are taken wildly out of context or simply insufficient to plead scienter. For instance, Plaintiff refers several times to Mr. Smith's supposed admissions that Equifax failed to take appropriate steps to prevent the Cybersecurity Incident. *E.g.* ¶ 64 ("Smith himself . . . admitted Equifax simply failed to 'have preventative measures in place to combat a data breach of this magnitude.'"); ¶ 182 ("Smith admitted" that the Cybersecurity Incident "occurred because 'basic [cybersecurity] hygiene issue wasn't followed.'"). But the first such "admission" consisted of no more than Mr. Smith making the tautological point to Congress that the existence

of the breach meant not "everything was -- was in place" to prevent it.[16] Similarly, the "basic hygiene" to which Mr. Smith referred in his Congressional testimony was the fact that the Apache Struts vulnerability at issue was not patched—which Defendants do not deny. Neither retrospective statement, however, comes close to an admission that Mr. Smith (or anyone else) *knew*, or was severely reckless in not knowing, that the specific vulnerability at issue in the Cybersecurity Incident had not been patched prior to data theft occurring.

Plaintiff also appears to try to equate the alleged facts that "one person was responsible for manually notifying the entire [IT] team about this critical vulnerability" (¶ 103) and that Equifax's system scanning depended upon such notification to seek out vulnerabilities (¶ 104) with scienter. But this claim again—that Equifax's security systems *must* have been inadequate because the Cybersecurity Incident occurred—does not establish that Defendants made false statements, much less knowingly or with severe recklessness. Moreover, Plaintiff's assertion that a single individual operated the entire patching process (¶ 65) is contrary to Mr. Smith's testimony (upon which the allegation is

[16] *Examining the Equifax Data Breach: Hearing Before the H. Financial Services Comm.*, 115th Cong. 120-121 (2017) (Testimony of Richard Smith, Former CEO, Equifax, Inc.), excerpts attached as Ex. G.

purportedly based), which instead made clear that the individual in charge of the patching process "had a team underneath him."[17]

Plaintiff's attempt to manufacture scienter from Mr. Smith's after-the-fact Congressional testimony that Equifax took post-Incident steps to improve security likewise fails, because that testimony has no bearing on Mr. Smith's state of mind at the time he made the challenged statements, prior to any post-Incident steps. Plaintiff fails to allege that Defendants knew Equifax's existing technology was so inadequate as to render general statements about Mr. Smith's and the Company's attention to data security false or severely reckless. *See, e.g.*, ¶ 105 (noting Equifax had upgraded its scanning technology); ¶ 184 (Equifax upgraded its security). Indeed, Plaintiff's assertion that the Company's data security measures were inadequate to prevent the Cybersecurity Incident hinges only on the fact that Cybersecurity Incident occurred. Such allegations fall far short of pleading scienter with any particularity.

---

[17] *Equifax: Continuing to Monitor Data-Broker Cybersecurity: Hearing Before the Sen. Subcomm. on Privacy, Technology and the Law of the Sen. Jud. Comm.*, 115th Cong. 15 (2017) (Testimony of Richard Smith, Former CEO, Equifax, Inc.), excerpts attached as Ex. H. Furthermore, Plaintiff's assertion that Equifax allegedly lacked an "inventory" of the software running on its system does not support an inference that Mr. Smith was aware of the need for, or lack of, such an inventory, and likewise insufficient to allege intent to defraud. *See* ¶¶ 103, 212.

3. Allegations of Defendants' Knowledge of the Cybersecurity Incident Do Not Support Scienter.

Plaintiff's allegations concerning Defendants' knowledge of the Cybersecurity Incident likewise fail to raise a strong inference of scienter as to any Individual Defendant. ¶¶ 272-75. As an initial matter, each challenged statement that Plaintiff attributes to Messrs. Gamble, Ploder, or Dodge—and all but one statement attributed to Mr. Smith—is alleged to have been made on or before July 27, 2017. *See generally* Statement Chart. However, ***Plaintiff affirmatively alleges that it was not until July 29, 2017—after all of these challenged statements***—that ***anyone*** at Equifax (much less any of the Individual Defendants) discovered that the hackers who orchestrated the Cybersecurity Incident had gained unauthorized access to the Company's network. ¶ 116. To adequately plead scienter, Plaintiff must allege facts establishing that a danger of misleading investors was "either known to the defendant or is so obvious that the defendant must have been aware of it" at the time the defendant spoke. *Mizzaro*, 544 F.3d at 1238. Plaintiff's allegation that ***no one at Equifax knew anything about the Cybersecurity Incident at the times these statements are alleged to have been made*** precludes any inference that the Defendants spoke with intent to deceive or the degree of *severe* recklessness required to plead scienter. *Id.*

Plaintiff's allegations are likewise insufficient to raise a strong inference of scienter as to the lone post-July 29, 2017 statement attributed to Defendant Smith. ¶ 334; Stmt. 22. During an August 17, 2017 speech at the University of Georgia's, Terry College of Business, Mr. Smith is alleged to have said: "when you have the size database we have, it's very attractive for others to try to get into our database, so it is a huge priority for us as you might guess. . . . [Data fraud] is my number one worry, obviously."[18] *Id.* Even assuming for argument's sake that Mr. Smith was aware that Equifax had suffered a significant cybersecurity attack at the time he is alleged to have made this statement (and Plaintiff fails to plead particular facts establishing that was so), such knowledge would not reasonably have suggested that it would be misleading to state that data security was a "huge priority" and his "number one worry," especially as his statements did not suggest that the Company was impervious to (or had not suffered) a security breach. *See Heartland*, 2009 WL 4798148, at *7 (finding scienter not adequately alleged where

[18] To be actionable under Section 10(b), a statement must have been made "in a manner reasonably calculated to influence the investing public[,]" such that it can be considered to have been made in connection with the purchase or sale of a security. *SEC v. Tex. Gulf Sulphur Co.*, 401 F.2d 833, 862 (2d Cir. 1968). Mr. Smith's speech at a Terry College of Business event (¶ 334) was not such a statement. *See http://www.terry.uga.edu/events/terry-third-thursday* ("Terry Third Thursday is a breakfast speaker series for the Atlanta business community that features influential speakers, as well as special guests from the University of Georgia, who bring local and global perspectives on business and innovation.").

plaintiff failed to plead facts supporting a strong inference that defendants knew statement of "emphasis on maintaining a high level of security" was false or misleading); *see also Mizzaro*, 544 F.3d at 1238 (scienter allegations must, at minimum, "present a danger of misleading buyers or sellers which is either known to the defendant or is so obvious that the defendant must have been aware of it").

The insufficiency of Plaintiff's allegations becomes all the more clear when considering the limited and incomplete knowledge Mr. Smith allegedly had about the Cybersecurity Incident as of August 17, 2017. The *most* Plaintiff alleges in this regard is that Mr. Smith had received a briefing (just two days earlier) "about Mandiant's conclusion" that "it appeared likely that consumer NPPI had been stolen." ¶ 122; *see also* ¶ 275. Plaintiff does not and cannot explain how it was purportedly misleading for Mr. Smith to make the statements he is alleged to have made on August 17, 2017 without simultaneously communicating this indefinite and incomplete interim alleged assessment from Mandiant.[19] It was fully

[19] Without citing any support, Plaintiff alleges Mr. Smith "admitted that Mandiant issued an August 11, 2017 report confirming that large amounts of consumer information had been compromised" in the Cybersecurity Incident. ¶ 275. In reality, Mr. Smith at no time testified or otherwise admitted that Mandiant issued a report of any kind on August 11, *see* Prepared Testimony of Richard F. Smith before the U.S. Senate Committee on the Judiciary, Subcommittee on Privacy, Technology and the Law, October 4, 2017 at 4. Mr. Smith instead clarified that, "[t]he first debriefing I had of any significance was on the 17th of August . . . that

appropriate, and prudent, for Equifax to continue its investigation and better understand the magnitude and scope of the Cybersecurity Incident before speaking publicly about it.[20] *Cf. Higginbotham v. Baxter Int'l, Inc.*, 495 F.3d 753, 760–61 (7th Cir. 2007) ("Prudent managers conduct inquiries rather than jump the gun with half-formed stories as soon as a problem comes to their attention . . . Taking the time necessary to get things right is both proper and lawful.")

4. Additional Scienter Allegations Fail to Support Scienter.

Plaintiff's allegations regarding the purported "egregiousness" of alleged "deficiencies in Equifax's cyber security practices" fail to raise a strong inference of scienter. ¶¶ 278-79. At best, these allegations criticize the Defendants in

---

included Mandiant." *Examining the Equifax Data Breach: Hearing Before the H. Financial Services Comm.*, 115th Cong. 109 (2017) (Testimony of Richard Smith, Former CEO, Equifax, Inc.) (excerpts attached as Ex. G), and that the speech he made on August 17th occurred *before* that meeting. *Oversight of the Equifax Data Breach: Answers for Consumers: Hearing Before the H. Subcomm. on Digital Commerce & Consumer Protection of the H. Comm. on Energy & Commerce*, 115th Cong. 30-31 (2017) (Testimony of Richard Smith, Former CEO, Equifax, Inc.) (excerpts attached as Ex. I). Plaintiff thus fails to allege the August 17, 2017 statements were false at all, much less knowingly or severely recklessly so.

[20] Based upon the already-discredited *Bloomberg* article, Plaintiff alleges that notifying Mr. Smith about the Cybersecurity Incident on July 31, 2017 meant the breach was "serious." ¶ 118. Plaintiff nowhere pleads facts establishing what Equifax considered a "serious" breach, nor how the fact of such a breach could render Mr. Smith's August 17, 2017 statements false, much less knowingly or recklessly so. Plaintiff's unattributed and unparticularized description of Equifax's supposed "protocol" should be disregarded.

hindsight for purportedly failing to effectively manage cybersecurity issues and prevent the Cybersecurity Incident. Such allegations do not even plead the actionable falsity of Defendants' statements, much less scienter. *See* Section III.A.1.a.; *see also Mogensen*, 15 F. Supp. 3d at 1218 (allegations that, at worst suggest poor business judgment, negligence, or mismanagement fail to adequately plead scienter); *Phillips v. LCI Int'l, Inc.*, 190 F.3d 609, 621 (4th Cir. 1999) (allegations which fail even to plead falsity of challenged statements "obviously" also fail to plead scienter); *accord In re Spectrum Brands, Inc. Sec. Litig.*, 461 F. Supp. 2d 1297, 1311-12 (N.D. Ga. 2006). Moreover, Plaintiff cannot rely on post-Cybersecurity Incident criticisms by media, purported "cybersecurity experts," and elected officials to establish a strong inference of scienter. *See In re Homebanc*, 706 F. Supp. 2d at 1360 ("Plaintiff's reliance upon after-the-fact events . . . amounts to little more than fraud by hindsight, which is not actionable.").

Allegations that cybersecurity was "critical to Equifax's business" and that Defendants had responsibility for and received updates regarding cybersecurity issues also fail to raise a strong inference of scienter. ¶¶ 276-77. Courts have repeatedly held that such generic allegations fail to plead scienter. *See, e.g.*, *Heartland*, 2009 WL 4798148, at *7 ("it is not automatically assumed that a corporate officer is familiar with certain facts just because these facts are important

to the company's business"); *Edward J. Goodman Life Income Tr. v. Jabil Circuit, Inc.*, 594 F.3d 783, 791 (11th Cir. 2010) (allegations of defendant's "responsibility to make decisions . . . fail[ed] to raise a strong enough inference of scienter"). Furthermore, Plaintiff's unremarkable allegations that Mr. Smith received briefings or periodic reports about cybersecurity, and discussed the issue at board meetings, offer no detail about the contents of such reports or discussions, including whether they informed him about the specific issues or vulnerabilities that allegedly contributed to the Cybersecurity Incident. *See* ¶¶ 51, 277. Plaintiff cites no company sources for these allegations (beyond Mr. Smith himself), and thus fails to plead that he was aware of anything that would contradict his public statements. *Thorpe v. Walter Inv. Mgmt. Corp.*, 111 F. Supp. 3d 1336, 1374 (S.D. Fla. 2015) (finding no strong inference of scienter where "Plaintiffs have not alleged with any particularity the contents of what [reports or other materials] Defendants…had access to" regarding the "true facts" of the company's issues and deficiencies).

Allegations that Mr. Smith and other Equifax employees resigned shortly after the Security Incident are not probative of a conscious or severely reckless effort to deceive investors. ¶¶ 280-82. These allegations do not suggest more than that Equifax and the executives in question concluded that their separation from the Company was appropriate "because the errors that le[d] to the [Cybersecurity

Incident] occurred on [those executives'] watch." *In re U.S. Aggregates, Inc. Sec. Lit*ig., 235 F. Supp. 2d 1063, 1073-74 (N.D. Cal. 2002); *see also N. Collier Fire Control & Rescue Dist. Firefighter Pension Plan v. MDC Partners, Inc.*, 2016 WL 5794774, at *21 (S.D.N.Y. Sept. 30, 2016) (holding that allegations about executive resignations failed to raise a strong inference of scienter).[21]

5. Alleged Stock Sales By Two Of Four Individual Defendants Do Not Support A Strong Inference Of Scienter.

Plaintiffs also attempt to raise an inference of scienter through allegations about sales of Equifax stock by Defendants Gamble and Ploder. As shown below, these allegations fail.

As an initial matter, Plaintiff's conspicuous failure to allege (much less challenge as purportedly "suspicious") *any* sales of Equifax stock by Mr. Smith or Mr. Dodge "overwhelms the inference" that Defendants "knowingly withheld from the public damaging and material information about" the company. *HomeBanc*,

[21] Plaintiff's related allegations that Equifax "publicly announc[ed] the possibility that Smith's conduct might satisfy the criteria for termination for 'cause,'" which allegedly requires "intentional or reckless misconduct," likewise fails to support scienter. ¶ 281. Plaintiff nowhere pleads that Equifax actually reclassified Mr. Smith's departure from "retirement" to "termination for cause," nor that it ultimately did "claw back" any of his compensation. *See id.* To the extent Equifax's determination of the nature of Mr. Smith's departure is relevant to the scienter inquiry—as Plaintiff apparently believes it should be—there is no allegation that Equifax has made any such decision.

706 F. Supp. 2d 1336; *see also Druskin v. Answerthink*, 299 F. Supp. 2d 1307, 1336 (S.D. Fla. 2004) ("The fact that the CEO, who held a significant amount of shares and who would have been an essential participant in any fraudulent scheme, did not sell stock undermines any suggestion of knowledge on the part of the defendants due to any other claimed insider sells."); *accord In re Coca-Cola Enters. Inc. Sec. Litig.*, 510 F. Supp. 2d 1187, 1202 (N.D. Ga. 2007) (lack of allegations of stock sales by CEOs undercut inference of scienter).

Nor do Plaintiff's allegations about sales made by Gamble and Ploder support any inference, much less a strong one, that these Defendants acted with scienter. The law is clear that alleged stock sales are not sufficient in and of themselves to support a strong inference of scienter. *See, e.g., In re Theragenics Corp. Sec. Litig.*, 105 F. Supp. 2d 1342, 1361-62 (N.D. Ga. 2000) (Thrash, J.). In order for such sales to contribute to an inference of scienter, Plaintiff must plead facts suggesting that the sales were motivated by knowledge of an impending decline in the stock's price. *Id.*; *accord In re Miller Indus., Inc. Sec. Litig.*, 12 F. Supp. 2d 1323, 1332 (N.D. Ga. 1998); *Coca-Cola Enters.*, 510 F. Supp. 2d at 1202. Plaintiff's allegations regarding sales of Equifax stock by Defendants Gamble and Ploder on August 1 and 2, 2017, respectively, fail this test and therefore do not support any inference of scienter. ¶¶ 283-84.

First, Plaintiff's allegations fail to establish either Defendant had any idea that Equifax's systems had been breached at the times they are alleged to have sold stock. Although Plaintiff alleges that *Mr. Smith* learned of some unauthorized access involving "credit 'dispute documents'" on July 31, 2017, Plaintiff does not allege that this, or anything about the Cybersecurity Incident, was communicated to Mr. Gamble prior to his August 1, 2017 sales, or to Mr. Ploder prior to his August 2, 2017 sales. ¶¶ 273-74.

Second, Plaintiff's allegations confirm that the August 2017 sales by Messrs. Gamble and Ploder were *not* the sort of "suspicious" sales that may be suggestive of scienter, given that these sales were small in comparison to both Defendants' sales during the entirety of the Class Period (which Plaintiff does not challenge as "suspicious"). *See* ¶ 283 (alleging that the August 2017 sales represented only about 20% of Mr. Ploder's sales and less than one third of Mr. Gamble's sales during the Class Period); *see also Theragenics*, 105 F. Supp. 2d at 1361 (noting that courts compare allegedly "suspicious" stock sales with prior trading activity to determine whether the allegedly "suspicious" sales suggest scienter).

If, as Plaintiff suggests, Messrs. Gamble and Ploder sold in early August 2017 because they had learned about the Cybersecurity Incident and feared that its announcement would cause Equifax's stock price to drop, one would expect to

have seen much larger sales by both Defendants relative to their prior trading (and their overall Equifax holdings). *See In re AFC Ent., Inc. Sec. Litig.*, 348 F. Supp. 2d 1363, 1374 (N.D. Ga. 2004) (observing that trading is "unusual" when "it is made at a time or in an amount that suggests that the seller is maximizing personal benefit from inside information"). That their August 2017 sales were relatively small by both measures suggests to the contrary that the sales were not motivated by these Defendants' possession of any such adverse nonpublic information. *Id*.[22]

6. Plaintiff Also Fails to Adequately Plead Scienter As to Equifax.

In evaluating whether Plaintiff has adequately pled Equifax's scienter, the Court must "look to the state of mind of the individual corporate official or officials who ma[d]e or issue[d] the statement[s]" Plaintiff challenges. *Mizzaro* 544 F.3d at 1254. Plaintiff's allegations fail to raise the required strong inference that any Individual Defendant acted with scienter, as shown above. As to the

[22] Although Plaintiff avoids acknowledging it in the Complaint, on November 3, 2017, Equifax publicly filed a Form 8-K with the SEC attaching the report of a Special Committee of Equifax directors who, with the assistance of respected and independent legal counsel, conducted a detailed investigation into the early August 2017 stock sales by Messrs. Gamble and Ploder, and found that neither had knowledge of the Cybersecurity Incident when their trades were made and that both Defendants had traded within the Company's permissible trading window, which had opened just days earlier. Ex. J. Plaintiff's failure to plead any facts disputing these publicly reported conclusions underscores Plaintiff's failure to properly allege that these stock sales are suggestive of scienter.

challenged statements not attributed to any Individual Defendant (Stmts. 1-6, 12-14, 22-23, 26; Statements Chart Tab G, the "Unattributed Statements"), Plaintiff's allegations fail to raise any inference, much less a strong one, that unnamed Equifax officials "were both responsible for issuing the allegedly false public statements and were aware of the alleged fraud." *Mizzaro* 544 F.3d at 1254-55. Plaintiff fails to adequately plead Equifax's scienter for this reason alone. *Id.*

Further, the Unattributed Statements are non-actionable aspirational statements about Equifax's "commitment" to data security or descriptions of then-existing data security standards and practices that have not been adequately pled as false. *See* Statement Chart Tab G; *see also* Section III.A. Plaintiff's failure to adequately allege that any of these statements were false or misleading when made (*see* Section III.A.) precludes any finding that Plaintiff has adequately pled scienter as to the statements. *See Phillips*, 190 F.3d at 621; *Spectrum Brand*s, 461 F. Supp. 2d at 1311-12.

C. Plaintiff Fails to Adequately Allege Loss Causation.

To plead loss causation, Plaintiff must allege facts demonstrating that a "corrective disclosure" that revealed the "truth" about a previous misstatement is responsible for a "substantial" amount of the price drops for which Plaintiff seeks to recover. *See Dura*, 544 U.S. at 345-48; *Meyer v. Greene*, 710 F.3d 1189, 1196-

97 (11th Cir. 2013). It is insufficient simply to allege a price decline following an announcement of negative information. *Meyer*, 710 F.3d at 1200 (stock drop following event that revealed no new information insufficient to plead loss causation). As shown below, Plaintiff fails to adequately plead loss causation.

The announcement of the Cybersecurity Incident on September 7, 2017 and related press coverage (¶ 355) did not "reveal" that prior statements referencing Equifax's commitment to data security, describing efforts to protect data and comply with applicable laws and regulations, and expressing opinions about data security and internal controls were false when made, and thus the announcement is not a corrective disclosure. *See* Section III.A.; *Dura*, 544 U.S. at 347; *accord Heartland*, 2009 WL 4798148, at *5; *Chipotle*, 2018 WL 1441373, at *22. It follows that the stock price decline allegedly following these disclosures is not indicative of loss caused by any alleged "fraud." *See Indiana State Dist. Council of Laborers & Hod Carriers Pension & Welfare Fund v. Omnicare, Inc.*, 583 F.3d 935, 944 (6th Cir. 2009) ("Although a number of allegations relate to Omnicare's alleged Part D shortcomings, none explain how the statements were revealed to be false and thereby caused a drop in the stock price.").

The alleged "revelations" on September 11, 2017—that Equifax purportedly lacked "an effective and comprehensive crisis management plan" to respond to the

Cybersecurity Incident and that "Congress was conducting a probe into [data security at] Equifax"—likewise fail to establish the falsity of any challenged statement or to plead loss causation. ¶ 357. Indeed, Plaintiff does not allege that Defendants made any misleading statement concerning Equifax's plans for managing a crisis such as the Cybersecurity Incident. *See Meyer*, 710 F.3d at 1197 (a corrective disclosure must at least "relate back to the misrepresentation and not to some other negative information about the company"). Further, this allegation again incorrectly attempts to convert allegations of purported mismanagement—here, the alleged lack of an "adequate" "crisis management" plan—into a Section 10(b) claim, in contravention of long-standing law. *See Santa Fe*, 430 U.S. at 479-80; *see also* Section III.A.1.a. Furthermore, news that Congress was investigating the Cybersecurity Incident did not reveal any prior statement to have been false. *See Meyer*, 710 F.3d at 1201 ("In our view, the commencement of an SEC investigation, without more, is insufficient to constitute a corrective disclosure for purposes of § 10(b).").

The alleged revelation on September 12, 2017 that 11.5 million consumers had signed up for the free TrustedID offering Equifax made available to consumers likewise fails to support loss causation. ¶ 358. Plaintiff does not explain how this report possibly could have revealed the falsity of any challenged statement; as

such, it is not "corrective" of alleged "fraud." *See FindWhat Investor Grp. v. FindWhat.com*, 658 F.3d 1282, 1311 n.28 (11th Cir. 2011) (observing that "a corrective disclosure must reveal a *previously concealed* truth"). Indeed, as Plaintiff's own allegations show, the announcement added no new and material information to what had previously been disclosed about the breach, given that (i) the Company had already announced on September 7, 2017 that at least 143 million consumers had been potentially impacted and (ii) concerns about the costs associated with responding to and remediating the Cybersecurity Incident were being discussed publicly. *See* ¶¶ 125, 129; *cf. FindWhat*, 658 F.3d at 1311 n.28 (observing that "a corrective disclosure must . . . disclose new information").

Plaintiff's allegations regarding information alleged to have come to light between September 13 and 14, 2017 likewise fail to support a finding that loss causation has been adequately pled. ¶ 359; *see also* ¶¶ 166-74. Plaintiff alleges that Equifax confirmed after the close of trading on September 13, 2017 that the specific vulnerability exploited in the Cybersecurity Incident was the Apache Struts weakness that was publicized in March 2017. ¶ 359. While Plaintiff contends this was new information about the Cybersecurity Incident, Plaintiff does not explain how this information revealed that any of the challenged statements were misleading. *See Chipotle*, 2018 WL 1441373, at *22 (holding that failures in

Chipotle's execution of food safety practices resulting in numerous outbreaks of illness failed to plead falsity of statements analogous to those challenged here); *In re Sec. Cap. Assurance Ltd. Sec. Litig*., 2011 WL 4444206, at *6 (S.D.N.Y. Sept. 23, 2011) (rating agency downgrades merely "highlighted the magnitude of the risk" and could not have "disclosed previously unknown subprime exposures"). Allegations that additional investigations by "Congressional committees and a coalition of state attorneys general" were announced on September 14, 2017 likewise did not "correct" any prior alleged fraudulent statements. *See Meyer*, 710 F.3d at 1201. Indeed, the most rational inference is that Equifax's stock price declined on September 14, 2017 due to concerns about the cost and impact of the additional investigations and continued negative publicity rather than as the result of a revelation of "fraud." *See Chipotle*, 2018 WL 1441373, at *29 n.9 (applying similar reasoning to analogous allegations); *see also Meyer*, 710 F.3d at 1196-97 (plaintiff should demonstrate that the fraudulent statement, and subsequent corrective disclosure, was a "'substantial' or 'significant' cause of the decline in price").

Finally, as discussed above, the resignation of certain Equifax officers and employees following the Cybersecurity Incident at best merely reflects a judgment that those persons' separation from the Company was appropriate "because the

errors that le[d] to the [Cybersecurity Incident] occurred on [their] watch." *U.S. Aggregates*, 235 F. Supp. 2d at 1073-74. As the resignation announcements did not "reveal some then-undisclosed fact with regard to the specific misrepresentations alleged in the complaint," these allegations fail to establish loss causation. *In re Omnicom Grp., Inc. Sec. Litig.*, 597 F.3d 501, 511 (2d Cir. 2010).

The Complaint fails to adequately plead loss causation and must be dismissed for this independent reason as well.

D. Plaintiff Fails to State a Section 20(a) Claim.

To allege a claim for control person liability under Section 20(a), a plaintiff must adequately plead that: (1) the company violated Section 10(b); (2) the defendant had the power to control the general affairs of the company; and, (3) the defendant had the power to control the specific corporate policy that resulted in the primary violation. *Theoharous v. Fong*, 256 F.3d 1219, 1227 (11th Cir. 2001). Plaintiff's failure to plead any primary violation of Section 10(b) by Equifax, alone, requires dismissal of the Section 20(a) claims as to each of the Individual Defendants. *See Mizzaro*, 544 F.3d at 1237; 15 U.S.C. § 78t(a).

Plaintiff also fails to adequately plead the Individual Defendants' control over the "specific corporate policy" that resulted in any alleged primary violation of Section 10(b) by Equifax. Plaintiff has not pled any Individual Defendant's

control over the "the content and dissemination of" the Unattributed Statements allegedly made on Equifax's website during the Class Period or of any challenged statement made by a different Individual Defendant. *See* Statement Chart (identifying statements attributed to particular Individual Defendants). Nor has Plaintiff specifically pled any Individual Defendant's control over the cybersecurity matters Plaintiff alleges were misrepresented. Finally, Plaintiff fails to adequately plead that Messrs. Gamble, Ploder, or Dodge controlled Equifax's "general affairs." *Theoharous*, 256 F.3d at 1227.

IV. CONCLUSION

For all of the foregoing reasons, the Court should grant Defendants' Joint Motion, and dismiss the Complaint for failure to state a claim.

DATED: June 7, 2018.

[signature block on next page]

KING & SPALDING LLP

/s /Michael R. Smith
Michael R. Smith
Georgia Bar Number: 661689
B. Warren Pope
Georgia Bar Number: 583723
Benjamin Lee
Georgia Bar Number: 443082
1180 Peachtree Street N.E.
Atlanta, GA 30309
Telephone: (404) 572-4600
Facsimile: (404) 572-5100
Email: mrsmith@kslaw.com
wpope@kslaw.com
blee@kslaw.com

Attorneys for Defendants Equifax Inc., John W. Gamble, Jr., Jeffrey L. Dodge, and Rodolfo O. Ploder

TROUTMAN SANDERS LLP

/s/ David M. Chaiken
David M. Chaiken
Georgia Bar No. 118618
600 Peachtree Street NE, Suite 3000
Atlanta, GA 30308
404-885-3000
404-885-3900 (Facsimile)
Email: david.chaiken@troutman.com

-and-

QUINN EMANUEL URQUHART & SULLIVAN, LLP
Steven G. Madison (admitted *pro hac vice*)
865 S. Figueroa Street, 10th Floor
Los Angeles, CA 90017
202-538-8000
Email: stevemadison@quinnemanuel.com

Michael E. Liftik (admitted *pro hac vice*)
Meghan A. McCaffrey (admitted *pro hac vice*)
1300 I Street, Suite 900
Washington, D.C. 20005
Telephone: (202) 538-8000
Email: michaelliftik@quinnemanuel.com
meghanmccaffrey@quinnemanuel.com

Attorneys for Defendant Richard F. Smith

LOCAL RULE 7.1(D) CERTIFICATION

Counsel hereby certifies that the text of this document has been prepared with Times New Roman 14 point font, one of the font and point selections approved by the Court in Local Rule 5.1(C).

/s/Michael R. Smith
Michael R. Smith
Georgia Bar No. 661689

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 7th day of June, 2018, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will send notice of the electronic filing to counsel of record.

/s/Michael R. Smith
Michael R. Smith
Georgia Bar No. 661689