IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

IN RE EQUIFAX INC. SECURITIES LITIGATION	CIVIL ACTION FILE NO. 17-CV-3463-TWT

OPINION AND ORDER

This is a securities fraud class action. It is before the Court on the Defendants' Joint Motion to Dismiss [Doc. 62]. For the reasons set forth below, the Defendants' Joint Motion to Dismiss [Doc. 62] is GRANTED in part and DENIED in part.

I. Background

This case arises out of a massive data breach incident. On September 7, 2017, the Defendant Equifax Inc. announced that it was the subject of a data breach affecting more than 148 million Americans (the "Data Breach").[1] Criminal hackers breached Equifax's Computer network and obtained a vast amount of personally identifiable information in the company's custody. The Lead Plaintiff, Union Asset Management Holding AG, seeks to represent a putative class of investors that purchased the securities of Equifax from February 25, 2016 through September 15, 2017. The Plaintiff alleges that the Defendants committed fraud in connection with the Data Breach that caused a

[1] Am. Compl. ¶ 3.

loss in value of the class's investments. Specifically, the Plaintiff alleges that the Defendants made multiple false or misleading statements and omissions about the sensitive personal information in Equifax's custody, the vulnerability of its internal systems to cyberattack, and its compliance with data protection laws and cybersecurity best practices.[2] Despite these assurances, Equifax allegedly failed to take some of the most basic precautions to protect its computer systems from hackers. According to the Plaintiff, these material misrepresentations artificially inflated the value of Equifax's securities, causing a loss in value of the class's investments when the truth was revealed after the Data Breach.

Equifax is a Georgia corporation with its headquarters in Atlanta, Georgia.[3] It is one of the three largest credit reporting agencies in the world.[4] Equifax operates primarily through four segments: U.S. Information Solutions, a segment that provides products and services to businesses; Equifax's International operating segment, which includes its Asia, Europe, Latin America, and Canada business units; Equifax's Workforce Solutions segment, which provides verification and employer services; and Global Consumer Solutions, its direct-to-consumer business that provides consumers with products to protect and monitor their credit and identity.[5] The Defendants

---

[2] *Id.* ¶ 3.

[3] *Id.* ¶ 19.

[4] *Id.*

[5] *Id.* ¶ 20.

Richard F. Smith, John W. Gamble, Jr., Rodolfo O. Ploder, and Jeffrey L. Dodge (the "Individual Defendants") were corporate officers at Equifax during the putative class period. The Defendant Richard F. Smith is the former Chief Executive Officer and Chairman of the Board of Directors of Equifax.[6] Smith resigned from both of these positions on September 26, 2017.[7] The Defendant John W. Gamble is the Corporate Vice President and Chief Financial Officer of Equifax.[8] The Defendant Rodolfo O. Ploder is the President of Equifax's Workforce Solutions operating segment.[9] The Defendant Jeffrey L. Dodge is the Senior Vice President of Investor Relations at Equifax.[10]

As part of its business, Equifax collects, maintains, and sells a huge quantity of personal data about consumers and employees all over the world.[11] This personally identifiable information is highly sensitive.[12] It includes Social Security numbers, addresses, birthdays, employment history, driver's license information, detailed payment history, loans, credit card information, and

---

6 *Id.* ¶ 21.

7 *Id.*

8 *Id.* ¶ 22.

9 *Id.* ¶ 23.

10 *Id.* ¶ 24.

11 *Id.* ¶ 29.

12 *Id.* ¶ 36.

more.[13] Credit bureaus such as Equifax acquire this information from banks, mortgage lenders, credit card issuers, and other financing companies.[14] This personally identifiable information is a highly valuable target for cybercriminals; it includes some of the most private information about consumers.[15] This information can be used to enter into a mortgage, set up a bank account, change a phone number, and even more.[16]

The Defendants recognized the importance of safeguarding this highly sensitive personal information.[17] In its SEC filings, Equifax acknowledged that it collected and stored sensitive data, including the personally identifiable information of consumers, and stated that safeguarding this data was "critical" to its "business operations and strategy."[18] It noted that its success was dependent upon its "reputation as a trusted steward of information."[19] Equifax also acknowledged that it was a valuable target for cybercriminals due to the vast trove of information it collected.[20] In its SEC filings, Equifax recognized

---

13 *Id.* ¶¶ 30, 36.

14 *Id.* ¶ 30.

15 *Id.* ¶ 36.

16 *Id.* ¶ 37.

17 *Id.* ¶ 38.

18 *Id.*

19 *Id.*

20 *Id.* ¶ 39.

that it was regularly the target of criminal hackers, and that a cybersecurity incident could subject it to a variety of serious consequences.[21]

Acknowledging the importance of protecting the data in its custody, the Defendants made a number of statements during the class period regarding Equifax's networks and the security of the personal data in its custody. According to the Plaintiff, the Defendants issued statements concerning the strength of Equifax's cybersecurity systems, its compliance with data protection laws, and the integrity of its internal controls.[22] For example, with regard to the strength of its data security, Equifax's website provided that the company employed "strong data security and confidentiality standards" and maintained "a highly sophisticated data information network that includes advanced security, protections and redundancies."[23] With regard to Equifax's compliance with data protection laws, regulations, and standards, the Defendants stated in SEC filings that they continuously monitored federal and state legislative and regulatory activities "in order to remain in compliance" with those laws.[24] The Defendants also certified in SEC filings during the class period that Equifax had effective internal controls that would provide "reasonable assurance regarding

---

21 *Id.*

22 *Id.* ¶ 52.

23 *Id.* ¶ 53.

24 *Id.* ¶ 277.

prevention or timely detection of unauthorized acquisition, use or disposition of our assets."[25]

However, despite these assurances, Equifax's cybersecurity was dangerously deficient. The Data Breach, according to the Plaintiff, was the inevitable result of widespread shortcomings in Equifax's data security systems. According to the Plaintiff's allegations, Equifax's data protection measures were "grossly inadequate," "failed to meet the most basic industry standards," and "ran afoul of the well-established mandates of applicable data protection laws."[26] These shortcomings spanned a number of facets of cybersecurity practices, including a failure to implement proper patching protocols, failure to encrypt sensitive information, the storage of sensitive data on public-facing servers, the use of inadequate network monitoring practices, the use of obsolete software, and more. Overall, according to cybersecurity experts, a "catastrophic breach of Equifax's systems was inevitable because of systemic organizational disregard for cybersecurity and cyber-hygiene best practices."[27]

According to the Plaintiff, Equifax failed to implement an adequate patch management process, while also failing to remediate known deficiencies in its cybersecurity infrastructure.[28] The company relied upon a single individual to

---

[25] *Id.* ¶ 62.

[26] *Id.* ¶ 208.

[27] *Id.* ¶ 66 (emphasis omitted).

[28] *Id.* ¶ 209.

manually implement its patching process across its entire network.[29] This individual had no way to know where vulnerable software in need of patching was being run on Equifax's systems.[30] This protocol was far less secure than the automatic patching processes that many other companies, including Equifax's peers, employ in their systems.[31] According to cybersecurity experts, this patching process fell far short of industry standards.[32]

Equifax also failed to encrypt sensitive data in its custody. According to the Amended Complaint, Equifax admitted that sensitive personal information relating to hundreds of millions of Americans was not encrypted, but instead was stored in plaintext, making it easy for unauthorized users to read and misuse.[33] Not only was this information unencrypted, but it also was accessible through a public-facing, widely used website.[34] This enabled any attacker that compromised the website's server to immediately have access to this sensitive personal data in plaintext.[35] Smith also admitted during congressional testimony that, with respect to its core credit databases, Equifax failed to

---

29 *Id.*

30 *Id.*

31 *Id.*

32 *Id.* ¶¶ 210-11.

33 *Id.* ¶ 217.

34 *Id.*

35 *Id.*

encrypt any of its data.[36] It also failed to encrypt its highly vulnerable mobile applications, meaning that in addition to keeping sensitive data unencrypted in its own systems, it also failed to encrypt data being transmitted over the internet.[37] This, according to experts, was a major security failure.[38] And, when Equifax did encrypt data, it left the keys to unlocking the encryption on the same public-facing servers, making it easy to remove the encryption from the data.[39] These inadequacies in Equifax's encryption protocol fell far short of industry standards and data security laws, and showed that Equifax did not "know what they were doing" with respect to data security.[40]

Moreover, Equifax also failed to implement adequate authentication measures.[41] Authentication measures are mechanisms, such as passwords, that verify that a party attempting to access a system or network is authorized to do so.[42] According to the Amended Complaint, Equifax's authentication measures were insufficient to protect the sensitive personal data in its custody from

---

36 *Id.*

37 *Id.* ¶ 218.

38 *Id.*

39 *Id.* ¶ 217.

40 *Id.* ¶¶ 218-19.

41 *Id.* ¶¶ 224-30.

42 *Id.* ¶ 224.

unauthorized access.[43] These mechanisms included weak passwords and security questions.[44] For example, Equifax relied upon four digit pins derived from Social Security numbers and birthdays to guard personal information, despite the fact that these weak passwords had already been compromised in previous breaches.[45] Furthermore, Equifax employed the username "admin" and the password "admin" to protect a portal used to manage credit disputes, a password that "is a surefire way to get hacked."[46] This portal contained a vast trove of personal information.[47] According to cybersecurity experts, these shortcomings demonstrated "poor security policy and a lack of due diligence."[48] Equifax's authentication practices fell short of the data security standards, which recommend the use of multi-factor authentication.[49]

Equifax also failed to adequately monitor its networks and systems, which greatly exacerbated the fallout of the Data Breach.[50] According to the Plaintiff, Equifax failed to establish mechanisms for monitoring its networks

---

43 *Id.*

44 *Id.*

45 *Id.*

46 *Id.* ¶ 225 (emphasis omitted).

47 *Id.*

48 *Id.*

49 *Id.* ¶ 226.

50 *Id.* ¶¶ 231-34.

and systems to alert when a threat existed.[51] Such mechanisms include maintaining activity logs, setting up processes for tracking malicious scripts, and implementing file integrity monitoring.[52] According to cybersecurity experts, logging is a "simple but crucial cybersecurity technique" in which a company monitors its systems by continuously logging network access so as to identify unauthorized users.[53] This failure by Equifax greatly compounded the magnitude of the Data Breach's impact. According to experts, a breach as large scale as this one would not have occurred if Equifax had implemented better monitoring systems. If adequate monitoring systems had been in place, Equifax could have identified the breach much earlier and prevented the exfiltration of consumer data from its network.[54] Improved logging techniques also could have enabled Equifax to expel the hackers from its systems and minimize the impact of the breach.[55] Instead, due in part to Equifax's failure to implement effective logging techniques, hackers were able to continuously access this sensitive personal data for over 75 days.[56] Equifax's failure to utilize proper network

---

51 *Id.* ¶ 231.

52 *Id.*

53 *Id.*

54 *Id.* ¶ 232.

55 *Id.*

56 *Id.*

monitoring, one of the most basic cybersecurity practices, demonstrates the fundamental deficiencies in its networks.[57]

Equifax's handling of the sensitive data in its custody also reflected a poor cybersecurity regime.[58] There were two main shortcomings as to this category. First, Equifax stored sensitive personal information, in unencrypted plaintext form, on public-facing servers and web portals.[59] Second, it failed to partition this sensitive information to limit the exposure if a breach occurred.[60] In contrast, standard security best practices recommend that companies ensure that sensitive data is stored on non-public servers and is inaccessible through public-facing networks.[61] Equifax's failure to properly segment its networks also contravened standard cybersecurity practices.[62] Experts note that network segmentation, which consists of dividing a network into smaller partitions, isolates critical assets from one another and controls the access to sensitive data.[63] Equifax's failure to properly handle this sensitive data is another example of the deficiencies in its cybersecurity regime.

---

57 *Id.* ¶ 233.

58 *Id.* ¶¶ 235-40.

59 *Id.* ¶ 235.

60 *Id.*

61 *Id.* ¶ 236.

62 *Id.* ¶ 237.

63 *Id.*

Many other aspects of Equifax's cybersecurity practices were also deficient. According to the Plaintiff, Equifax relied upon outdated security systems and software,[64] allowed its "attack surface" to grow too big by leaving thousands of servers exposed on the internet;[65] allowed unused data to accumulate and failed to dispose of unneeded data;[66] failed to restrict access to sensitive data to only those employees whose job responsibilities required such access;[67] failed to adequately train its security personnel;[68] failed to perform adequate reviews of its systems, networks, and security;[69] and failed to develop a data breach management plan.[70] However, despite the woeful state of Equifax's cybersecurity, the Defendants made a number of statements touting the strength of Equifax's data systems and the cybersecurity practices that it employed.[71]

According to the Plaintiff, the Defendants also ignored a number of warnings that Equifax's data security measures were inadequate. In 2014,

---

64 *Id.* ¶¶ 241-45.

65 *Id.* ¶¶ 246-47.

66 *Id.* ¶¶ 248-50.

67 *Id.* ¶¶ 251-53.

68 *Id.* ¶¶ 254-60.

69 *Id.* ¶¶ 261-63.

70 *Id.* ¶¶ 264-66.

71 *Id.* ¶¶ 285-353.

KPMG performed a security audit of Equifax which found that, among other deficiencies, Equifax left encryption keys on the same public servers where encrypted data was stored.[72] Then, in 2016, Equifax hired Deloitte to perform another security audit.[73] Deloitte discovered several problems in its audit, including inadequate patching systems.[74] However, according to former cybersecurity employees at Equifax, the company's management did not take the security audit seriously.[75] Equifax employees and cybersecurity researchers continued to warn Equifax of deficiencies in its cybersecurity protocol.[76] They warned Equifax about its inadequate patching systems, its failure to encrypt sensitive personal data, its storage of personal data on public-facing servers, and more.[77] Furthermore, in March 2017, Equifax hired Mandiant, a cybersecurity firm, to investigate weaknesses in its data protection systems.[78] This investigation, which was described as a "top-secret project," was personally overseen by Smith.[79] Mandiant concluded that Equifax's data protection systems

---

72 *Id.* ¶ 71.

73 *Id.* ¶ 77.

74 *Id.*

75 *Id.*

76 *Id.* ¶¶ 78-83.

77 *Id.*

78 *Id.* ¶ 91.

79 *Id.*

were grossly inadequate.[80] Mandiant specifically identified Equifax's unpatched systems and "misconfigured security policies" as indicative of major problems.[81] However, instead of heeding Mandiant's advice, Equifax squelched a broader review of Equifax's security systems.[82]

Equifax also experienced other, smaller data breaches prior to the Data Breach here. According to the Plaintiff, these previous breaches should have warned the Defendants that Equifax's cybersecurity, including its authentication and network monitoring measures, was severely deficient. In April 2016, hackers breached Equifax's W2Express website, a service that offers downloadable W-2 forms for companies.[83] The hackers were able to access the W-2 data of hundreds of thousands of employees of numerous companies that contracted with Equifax to use this service.[84] The hackers were able to access this information by entering an employee's default PIN code, which was the last four digits of the employee's Social Security number and their four-digit birth year.[85] According to cybersecurity experts, these authentication measures fell

---

80 *Id.* ¶ 92.

81 *Id.*

82 *Id.* ¶ 93.

83 *Id.* ¶ 73.

84 *Id.*

85 *Id.*

short of data security best practices.[86] The hackers were also able to remain undetected in Equifax's networks for approximately one year before they were discovered, which the Plaintiff alleges reflected a failure to employ adequate network monitoring practices.[87] Then, in February 2017, Equifax learned that another breach occurred in its Workforce Solutions segment.[88] From April 2016 to March 2017, hackers were able to obtain wage and W-2 data maintained by Equifax's TALX division, now called Equifax Workforce Solutions.[89] The hackers were again able to exploit Equifax's use of personal identifiers and weak four-digit PIN codes to protect this sensitive data.[90] The hackers also were able to remain in Equifax's network for over a year.[91] Cybersecurity experts opined that Equifax's authentication protections, which were exploited in this breach, were inadequate and failed to meet basic industry standards.[92] After this incident Equifax promised to make improvements in its cybersecurity defenses, but failed to do so.[93]

---

86 *Id.*

87 *Id.* ¶ 73.

88 *Id.* ¶ 85.

89 *Id.*

90 *Id.*

91 *Id.* ¶ 87.

92 *Id.* ¶ 89.

93 *Id.* ¶ 90.

On or about March 7, 2017, security firms began issuing warnings that attackers were exploiting a vulnerability in Apache Struts, an open-source software application used to build interactive websites.[94] This software is commonly used for websites where customers submit online forms.[95] Apache Struts is widely used by large businesses, including a substantial percentage of the Fortune 100 companies.[96] Equifax used Apache Struts at this time. Security firms began reporting that Apache Struts was vulnerable to a "remote code execution attack."[97] This attack is a dangerous type of exploit that allows attackers to force the vulnerable systems into running computer programs written by the attackers, which can make it easy to either steal data or establish a foothold in the vulnerable system.[98] This weakness in Apache Struts was not just highly dangerous – it was also especially easy to exploit.[99] Due to both the dangerous nature of this vulnerability and the widespread use of Apache Struts in the business community, the vulnerability and the corresponding update to the software aimed at addressing the vulnerability were widely publicized.[100]

---

94 *Id.* ¶ 95.

95 *Id.*

96 *Id.*

97 *Id.* ¶ 96.

98 *Id.*

99 *Id.*

100 *Id.* ¶ 97.

Both Apache itself and security firms publicized the vulnerability.[101] By March 8, 2017, Apache released updated versions of Apache Struts to mitigate this vulnerability in the software.[102]

In March 2017, hackers breached Equifax's network using the Apache Struts vulnerability.[103] On or about May 13, 2017, the hackers accessed files containing Equifax usernames and passwords, which they then used to access documents and sensitive information in Equifax's "legacy environment," an area where it stored old data that it no longer used.[104] The attackers accessed numerous databases and compromised multiple systems.[105] The collection of information that the hackers obtained was so large that they had to break it up into smaller pieces to avoid setting off alarms.[106] The hackers ultimately stole the names, Social Security numbers, birthdays, addresses, drivers license information, tax identification numbers, and other personal data of 148 million Americans, as well as personal information of nearly one million foreign

---

101 *Id.*

102 *Id.* ¶ 98.

103 *Id.* ¶¶ 109-10.

104 *Id.* ¶ 112.

105 *Id.* ¶ 113.

106 *Id.* ¶ 114.

consumers and employees.[107] They also obtained the credit card information for 209,000 consumers.

On July 29 and 30 of 2017, Equifax discovered that criminal hackers had gained unauthorized access to its network.[108] Susan Mauldin, Equifax's Chief Security Officer, notified John Kelly, Equifax's Chief Legal Officer, about the Data Breach on July 31.[109] Mauldin informed Kelly that personally identifiable information may have been compromised in the Data Breach.[110] Under Equifax's data security protocol, the chief of security is alerted about any issues, who then determines the severity of the breach.[111] If the chief of security determines the breach to be severe, he or she then informs the executive leadership of the issue.[112] On July 31, Smith was notified about the Data Breach.[113] Kelly told Smith that Chief Information Officer David Webb would meet with him in person to discuss a data security issue.[114] In this meeting, Webb notified Smith

---

107 *Id.* ¶ 115.

108 *Id.* ¶ 116.

109 *Id.* ¶ 117.

110 *Id.*

111 *Id.* ¶ 118.

112 *Id.*

113 *Id.* ¶ 118.

114 *Id.*

of the Data Breach, informing him that it had occurred in an online consumer dispute portal.[115]

On August 2, 2017, Equifax notified the FBI of the Data Breach.[116] It also retained legal counsel to guide its investigation into the breach.[117] The same day, Equifax's legal counsel retained Mandiant to assist in the investigation into the incident.[118] Experts would later note that these steps suggested that Equifax knew that the Data Breach was serious.[119] In the days immediately following the discovery of the Data Breach, Gamble and Ploder sold more than $1 million in Equifax stock.[120] On August 1, Gamble, Equifax's Chief Financial Officer, sold stock for $946,374, representing more than thirteen percent of his holdings.[121] On August 2, Ploder sold stock for $250,458, representing four percent of his holdings.[122] These sales were not made pursuant to a Rule 10b5–1 trading plan.[123] Smith would later state in congressional testimony that Ploder and

---

115 *Id.* ¶ 119.

116 *Id.* ¶ 120.

117 *Id.*

118 *Id.*

119 *Id.*

120 *Id.* ¶ 121.

121 *Id.*

122 *Id.*

123 *Id.*

Gamble would have been in many of the meetings he had concerning the Data Breach.[124]

By August 11, 2017, Mandiant confirmed that hackers accessed databases containing a large amount of consumers' personally identifiable information.[125] Smith requested a briefing on the Data Breach on August 15, 2017.[126] At this briefing, Smith was informed that it was likely that personally identifiable information had been stolen.[127] On August 16, 2017, at an Equifax investor conference, the Defendants stated that Equifax's "role as a Trusted Steward is a Key Execution Enabler" and stated that it was making "investments to address critical data security throughout the company."[128] On August 17, 2017, Smith spoke at an event at the Terry College of Business at the University of Georgia.[129] When asked by an audience member how Equifax prepares for data fraud, Smith responded "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

---

124 *Id.*

125 *Id.* ¶ 122.

126 *Id.*

127 *Id.*

128 *Id.* ¶ 123.

129 *Id.* ¶ 334.

as you might guess. [] [Data fraud] is my number one worry, obviously."[130]

On September 7, 2017, Equifax disclosed the Data Breach to the public for the first time.[131] In a press release after the close of trading that day, Equifax revealed that it had suffered a data breach affecting the personal information of approximately 143 million American consumers.[132] Equifax continued to make subsequent disclosures over the following days, ending on September 15, 2017, providing additional details concerning the Data Breach.[133] The company stated that it had engaged Mandiant, a cybersecurity firm, to conduct a review, and that it had reported the breach to law enforcement.[134] Experts, analysts, and the media immediately began to weigh in, with one analyst describing the breach as "one of the biggest cyber-attacks in US history."[135] Cybersecurity experts opined that massive cybersecurity failures on Equifax's part resulted in the Data Breach, and that its public response and outreach were "haphazard and ill-conceived."[136] Financial experts also began to weigh in. Some financial

---

130 *Id.* This speech was recorded and uploaded to YouTube.com on August 22, 2017.

131 *Id.* ¶ 124.

132 *Id.* ¶ 125.

133 *Id.* ¶ 124.

134 *Id.* ¶ 126.

135 *Id.* ¶ 128.

136 *Id.* ¶ 131.

analysts predicted from the outset of this public revelation that, due to the unprecedented size of this incident, Equifax's stock price would decline.[137] Other analysts predicted that Equifax would incur substantial costs relating to the Data Breach for years to come.[138]

On September 8, 2017, the price of Equifax's common stock dropped nearly fifteen percent, closing at $123.13 per share.[139] There was also an extraordinarily high trading volume of 16.85 million shares of Equifax stock.[140] On Monday, September 11, 2017, in response to more revelations made over the weekend, Equifax's stock price fell another nine percent to $113.32 per share.[141] Over the course of the next few days, more information concerning Equifax's cybersecurity and the Data Breach was revealed to the public.[142] By September 15, 2017, Equifax's stock price had fallen to $92.98, nearly a thirty-six percent decline since the initial public disclosure of the Data Breach.[143]

On September 8, 2017, this action was commenced. In the Amended Complaint, the Plaintiff asserts one claim for violation of section 10(b) of the

---

137 *Id.* ¶ 128.

138 *Id.* ¶ 129.

139 *Id.* ¶ 138.

140 *Id.*

141 *Id.* ¶ 151.

142 *Id.* ¶¶ 154-79.

143 *Id.* ¶ 177.

Exchange Act and Rule 10b–5 promulgated thereunder against all of the Defendants (Count I), and one claim for violation of section 20(a) of the Exchange Act against the Individual Defendants (Count II). The Plaintiff alleges that the Defendants made false or misleading statements on Equifax's website, in Equifax's SEC filings, and at Equifax Investor Conferences and Presentations. According to the Plaintiff, these false or misleading statements concerned the state of Equifax's cybersecurity, Equifax's compliance with data protection laws, regulations, and industry best practices, and Equifax's internal controls. On June 18, 2018, this Court modified the PSLRA's automatic stay of discovery to allow for limited case management and discovery planning activities.[144] The Defendants now move to dismiss.

II. Legal Standard

A complaint should be dismissed under Rule 12(b)(6) only where it appears that the facts alleged fail to state a "plausible" claim for relief.[145] A complaint may survive a motion to dismiss for failure to state a claim, however, even if it is "improbable" that a plaintiff would be able to prove those facts; even if the possibility of recovery is extremely "remote and unlikely."[146] In ruling on a motion to dismiss, the court must accept the facts pleaded in the complaint as

---

144 *See* [Doc. 64].

145 *Ashcroft v. Iqbal*, 129 S. Ct. 1937, 1949 (2009); FED. R. CIV. P. 12(b)(6).

146 *Bell Atlantic v. Twombly*, 550 U.S. 544, 556 (2007).

true and construe them in the light most favorable to the plaintiff.[147] Generally, notice pleading is all that is required for a valid complaint.[148] Under notice pleading, the plaintiff need only give the defendant fair notice of the plaintiff's claim and the grounds upon which it rests.[149]

Complaints that allege fraud under federal securities law must satisfy the heightened pleading requirements of both Rule 9(b) and the Private Securities Litigation Reform Act of 1995. Rule 9(b) requires a complaint to "state with particularity the circumstances constituting fraud."[150] "A complaint satisfies Rule 9(b) if it sets forth precisely what statements or omissions were made in what documents or oral representations, who made the statements, the time and place of the statements, the content of the statements and manner in which they misled the plaintiff, and what benefit the defendant gained as a consequence of the fraud."[151]

---

[147] *See Quality Foods de Centro America, S.A. v. Latin American Agribusiness Dev. Corp., S.A.*, 711 F.2d 989, 994-95 (11th Cir. 1983); *see also Sanjuan v. American Bd. of Psychiatry and Neurology, Inc.*, 40 F.3d 247, 251 (7th Cir. 1994) (noting that at the pleading stage, the plaintiff "receives the benefit of imagination").

[148] *See Lombard's, Inc. v. Prince Mfg., Inc.*, 753 F.2d 974, 975 (11th Cir. 1985), *cert. denied*, 474 U.S. 1082 (1986).

[149] *See Erickson v. Pardus*, 551 U.S. 89, 93 (2007).

[150] FED. R. CIV. P. 9(b).

[151] *In re Theragenics Corp. Sec. Litig.*, 105 F. Supp. 2d 1342, 1348 (N.D. Ga. 2000) (citing *Brooks v. Blue Cross and Blue Shield of Fla., Inc.*, 116 F.3d 1364, 1371 (11th Cir. 1997)).

The PSLRA also sets forth heightened pleading standards. This law was "enacted to cure perceived abuses in prosecuting class actions brought pursuant to federal securities laws."[152] The PSLRA supplements Rule 9(b) in two ways. First, a plaintiff must specify "the reason or reasons why the statement is misleading, and, if an allegation regarding the statement or omission is made on information and belief, the complaint shall state with particularity all facts on which that belief is formed."[153] Second, a plaintiff must set forth particular facts that give rise to a strong inference that the defendants acted with the required state of mind.[154] Specifically, it requires that "the complaint shall, with respect to each act or omission alleged to violate this chapter, state with particularity facts giving rise to a strong inference that the defendant acted with the required state of mind."[155] A complaint that fails to comply with any of these requirements must be dismissed.[156]

III. Discussion

Section 10(b) of the Exchange Act of 1934 makes it unlawful "[t]o use or employ, in connection with the purchase or sale of any security . . . any

---

[152] *In re Scientific–Atlanta, Inc., Sec. Litig.*, 239 F. Supp. 2d 1351, 1358 (N.D. Ga. 2002).

[153] 15 U.S.C. § 78u–4(b)(1).

[154] 15 U.S.C. § 78u–4(b)(2).

[155] 15 U.S.C. § 78u–4(b)(2).

[156] 15 U.S.C. § 78u–4(b)(3)(A).

manipulative or deceptive device or contrivance in contravention of such rules and regulations as the Commission may prescribe."[157] Rule 10b–5, promulgated thereunder by the Commission, states:

> It shall be unlawful for any person, directly or indirectly, by use of any means or instrumentality of interstate commerce, or of the mails or of any facility of any national securities exchange, (a) To employ any device, scheme, or artifice to defraud, (b) To make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading, or (c) To engage in any act, practice, or course of business which operates or would operate as a fraud or deceit upon any person, in connection with the purchase or sale of any security.[158]

To establish a securities fraud claim under these provisions, a plaintiff must 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, commonly called 'loss causation.'"[159]

The Defendants make four main arguments. First, they argue that the Plaintiff has failed to adequately plead that they made false or misleading statements. Second, they contend that the Plaintiff has failed to plead a strong

---

[157] 15 U.S.C. § 78j(b).

[158] 17 C.F.R. § 240.10b–5.

[159] *Mizzaro v. Home Depot, Inc.*, 544 F.3d 1230, 1236-37 (11th Cir. 2008).

inference of scienter, as required under the PSLRA. Third, they argue that the Plaintiff fails to adequately plead loss causation, an essential element of a section 10(b) claim. Finally, they argue that the Plaintiff's section 20(a) claim fails. The Court addresses each of these arguments in turn.

A. False or Misleading Statements

The Defendants first argue that the Plaintiff fails to sufficiently plead that the statements in question were false or misleading, as required by the PSLRA.[160] Complaints alleging fraud must meet the heightened-pleading standards of Rule 9(b), which requires that in "alleging fraud or mistake, a party must state with particularity the circumstances constituting fraud or mistake."[161] A fraud claim meets the requirements of Rule 9(b) if it sets forth precisely what statements or omissions were made in what documents or oral presentations, who made the statements, the time and place of the statements, the contents of the statements or manner in which they misled the plaintiff, and what the defendants gained as a consequence.[162] Additionally, the PSLRA requires a securities-fraud plaintiff to "specify each statement alleged to have been misleading" and "the reason or reasons why the statement is

---

160 Defs.' Mot. to Dismiss, at 9.

161 FED. R. CIV. P. 9(b).

162 *Brooks v. Blue Cross and Blue Shield of Fla.*, 116 F.3d 1364, 1371 (11th Cir.1997).

misleading."[163] "To show falsity, one typically juxtaposes an alleged misrepresentation to a contrary true fact."[164] "A statement is misleading if in the light of the facts existing at the time of the statement a reasonable investor, in the exercise of due care, would have been misled by it."[165] If an allegation regarding a statement or omission is made on information and belief, the complaint must state with particularity the facts on which the belief is formed.[166]

This securities-fraud case is based primarily on the Defendants' alleged misrepresentations during the class period about the security of Equifax's networks and its efforts to ensure the protection of the data in its custody. The Defendants' purported misrepresentations can be grouped into three main categories: (1) statements concerning Equifax's cybersecurity and its efforts to protect consumer data; (2) statements concerning Equifax's compliance with data protection laws, regulations, and industry best practices; and (3) statements concerning Equifax's internal controls. The Defendants make four main arguments in favor of dismissal. First, they argue that many of the Plaintiff's claims allege mere corporate mismanagement. Second, they argue

---

[163] 15 U.S.C. § 78u–4(b)(1).

[164] *In re HomeBanc Corp. Sec. Litig.*, 706 F. Supp. 2d 1336, 1353 (N.D. Ga. 2010).

[165] *FindWhat Inv. Grp. v. FindWhat.com*, 658 F.3d 1282, 1305 (11th Cir. 2011) (internal quotations and alterations omitted).

[166] *Id.*

that the Plaintiff has not sufficiently pleaded the falsity of the alleged statements as required by the PSLRA. Third, they argue alleged statements of opinion or belief are not actionable. Fourth, they argue that they were under no duty to disclose the Data Breach prior to September 7, 2017. The Court addresses each of these.

1. Corporate Mismanagement

The Defendants first contend that many of the Plaintiff's allegations concern mere corporate mismanagement, which is not actionable under the federal securities laws.[167] Specifically, the Defendants contend that "[a]llegations 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."[168] In *Santa Fe Industries, Inc. v. Green*, the Supreme Court held that allegations of corporate mismanagement are not actionable under section 10(b) because the federal securities laws do not regulate corporate fiduciary duties.[169] There, the Supreme Court rejected a minority shareholder's claim that the company's majority shareholders violated

---

167 Defs.' Mot. to Dismiss, at 12-13.

168 *Id.*

169 *Santa Fe Indus., Inc. v. Green*, 430 U.S. 462, 477 (1977) ("No doubt Congress meant to prohibit the full range of ingenious devices that might be used to manipulate securities prices. But we do not think it would have chosen this 'term of art' if it had meant to bring within the scope of s 10(b) instances of corporate mismanagement such as this, in which the essence of the complaint is that shareholders were treated unfairly by a fiduciary.").

section 10(b) by utilizing a short-form merger to eliminate the minority's interest.[170] The Court concluded that the transaction at issue was not manipulative or deceptive within the meaning of section10(b), and consequently not actionable.[171] Thus, a plaintiff who alleges mere corporate mismanagement or breach of fiduciary duty does not state a claim under section10(b). From this, the Defendants argue that many of the Plaintiff's claims fail because they merely make hindsight criticisms of the adequacy of Equifax's management of its data security efforts.

"However, 'false or misleading statements or omissions concerning material facts about management or internal operations may be actionable,' such as when a defendant 'makes certain statements while that defendant knows that existing mismanagement makes those statements false or misleading.'"[172] Thus, while allegations that Equifax engaged in mismanagement would fail under section 10(b), allegations that the Defendants made false or misleading statements or omissions concerning such corporate mismanagement at Equifax can constitute basis for a section 10(b) claim.[173] The

---

[170] *Id.* at 465.

[171] *Id.* at 465, 473.

[172] *In re Ebix, Inc. Sec. Litig.*, 898 F. Supp. 2d 1325, 1340 (N.D. Ga. 2012) (quoting *In re Premiere Techs. Inc.*, No. 1:98-CV-1804-JOF, 2000 WL 33231639, at *14 (N.D. Ga. Dec. 8, 2000)).

[173] The Defendants cite cases for the proposition that misstatements concerning corporate mismanagement, along with allegations of corporate mismanagement, are *also* not cognizable under the federal securities

Defendants misconstrue the Plaintiff's argument. The Plaintiff does not argue that the Defendants violated section 10(b) by failing to implement better cybersecurity practices. Instead, the Plaintiff contends that the Defendants violated section 10(b) by making false or misleading statements as to the strength and quality of Equifax's cybersecurity. Such a claim is not barred by *Santa Fe*.

2. The Adequacy of Equifax's Data Security

Next, the Defendants argue that the statements touting the strength of Equifax's data security systems and the adequacy of Equifax's efforts to promote cybersecurity do not constitute material misrepresentations. In the Amended Complaint, the Plaintiff alleges that the Defendants made a variety of material

---

laws/section 10(b). *See* Defs.' Mot. to Dismiss, at 13 (citing *Cutsforth v. Renschler*, 235 F. Supp. 2d 1216, 1242-44 (M.D. Fla. 2002)). However, the Supreme Court's holding in *Santa Fe* does not support such a conclusion, and the cases cited are not binding authority on this Court. The Court instead agrees with the courts in this District that have concluded that false or misleading statements or omissions concerning corporate mismanagement are cognizable under the federal securities laws. *See, e.g.*, *In re Ebix, Inc. Sec. Litig.*, 898 F. Supp. 2d 1325, 1340 (N.D. Ga. 2012). The Defendants cite *Cutsforth v. Renschler* for the proposition that a failure to disclose mismanagement is also not cognizable under the federal securities laws. The Court finds the reasoning in *Cutsforth* and similar cases unconvincing. In those cases, the courts do not explain why nondisclosure of mismanagement is inactionable under *Santa Fe*. Furthermore, the facts of those cases are distinguishable. The court in *Cutsforth* found that the mere nondisclosure of mismanagement itself was not actionable. In contrast, the Plaintiff here alleges that the Defendants made affirmative *misstatements* concerning mismanagement of cybersecurity, not a mere failure to disclose. Even applying the holding in *Cutsforth* and similar cases, such misstatements would be actionable. Thus, the Court also finds that *Cutsforth* is distinguishable.

misrepresentations as to the state of Equifax's data security and Equifax's efforts to promote cybersecurity. For example, the Defendants allegedly stated that Equifax was a "trusted steward" of personal data and that it employed "strong data security and confidentiality standards on the data that we provide and on the access to that data."[174] They allegedly stated that Equifax "maintain[ed] a highly sophisticated data information network that includes advanced security, protections and redundancies."[175] According to the Plaintiff, the fundamental shortcomings in Equifax's cybersecurity, including a failure to take some of the most elementary precautions, render these statements false or misleading.[176]

The Defendants make two main arguments for why these statements are not material misrepresentations. First, they argue that the alleged statements are not actually false or misleading because the facts pleaded do not show that Equifax's data security was actually inadequate. Second, they contend that these statements constitute inactionable puffery. According to the Defendants, these statements were vague, meaningless, statements of corporate optimism that no reasonable shareholder would rely upon in making investment decisions. The Court addresses each of these arguments in turn.

---

174 Am. Compl. ¶ 289.

175 *Id.*

176 Pl.'s Br. in Opp'n to Defs.' Mot. to Dismiss, at 16.

i. Falsity

The Defendants contend that the Plaintiff has failed to plead the falsity of each of the alleged statements concerning the strength of Equifax's systems. They argue that the Plaintiff has not shown that the statements boasting of the strength and complexity of Equifax's cybersecurity are actually false.[177] Instead, according to the Defendants, the Plaintiff has only alleged that Equifax was the victim of a criminal attack that was out of its control. They contend that the fact that a company suffered a significant cyberattack does not necessarily mean that its cybersecurity was deficient, and thus does not render its prior statements about its commitment to data security false.[178]

However, the Plaintiff alleges more than just the mere occurrence of the Data Breach. The Plaintiff has pleaded a multitude of specific, detailed factual allegations demonstrating that Equifax's cybersecurity systems were grossly deficient and outdated, despite the Defendants' various assurances to the contrary. In the Amended Complaint, the Plaintiff alleges that Equifax failed to implement even the most basic security measures, reflecting a "systemic organizational disregard for cybersecurity and cyber-hygiene best practices."[179] Cybersecurity experts opined that Equifax's data security failures flowed from

---

177 Defs.' Mot. to Dismiss, at 13-15.

178 *Id.* at 15.

179 Am. Compl. ¶ 66.

an inadequate "tone at the top" and that "the real problem was a very poor focus on information security at the highest levels of the company."[180] For example, according to the Plaintiff, Equifax failed to implement an effective patch management process, relying upon a single employee to manually implement the company's patching process across its entire network.[181] This process failed to meet the most basic industy standards – application of security patches is a critical cybersecurity practice.[182] Because of this shortcoming, Equifax allegedly failed to remediate known deficiencies in its cybersecurity infrastructure, such as the Apache Struts vulnerability.[183] Furthermore, according to the Plaintiff, Equifax failed to implement adequate encryption measures to protect sensitive information, in contrast to its representation that it encrypted confidential information.[184] Equifax allegedly stored and transmitted the personal information of hundreds of millions of consumers in unencrypted, plaintext, making it easy for intruders to read and misuse.[185]

Overall, the Plaintiff alleges that, among other things, Equifax: (1) failed to implement adequate patching processes; (2) failed to create adequate

---

180 *Id.* ¶ 257.

181 *Id.* ¶ 209.

182 *Id.* ¶ 210.

183 *Id.* ¶ 209.

184 *Id.* ¶¶ 65, 217-23, 295.

185 *Id.* ¶ 65.

encryption measures to protect the information in its custody; (3) failed to implement adequate authentication measures to ensure that parties attempting to access its networks were authorized to do so; (4) failed to establish mechanisms for monitoring its networks for security breaches; (5) stored personal data in easily accessible public channels; (6) relied on outdated and obsolete software; and (7) failed to warehouse obsolete personal information.[186] Together, according to the Plaintiff, each of these shortcomings created an inadequate cybersecurity system.

Given the dangerously deficient state of Equifax's cybersecurity, the Court concludes it was false, or at least misleading, for Equifax to tout its advanced cybersecurity protections. In contrast to the Defendants' representations that, among other things, Equifax employed a "highly sophisticated data information network" and "advanced security protections,"[187] Equifax's data security was dangerously lacking. While it is true that the mere occurrence of a data breach may not necessarily mean that a company's data security systems are inadequate, the Plaintiff here does not rely solely upon the occurrence of the Data Breach to establish that the Defendants' statements were false. Instead, the Plaintiff has pleaded a variety of facts showing that Equifax's

---

186 *Id.* ¶ 65.

187 *Id.* ¶ 289.

cybersecurity systems were outdated, below industry standards, and vulnerable to cyberattack, and that Equifax did not prioritize data security efforts.

Furthermore, as the Plaintiff points out, a number of courts have come to a similar conclusion, holding that statements touting the strength or quality of an important business operation are false, and thus actionable, when those operations are, in reality, deficient.[188] For example, in *In re ValuJet, Inc., Securities Litigation* the court explained that:

> The Plaintiffs allege that, despite the numerous safety-related incidents and FAA heightened scrutiny of ValuJet's operations, (1) Defendants Jordon and Priddy fraudulently represented in the 1995 report to shareholders that ValuJet's paramount goal was profitability while maintaining operational integrity; (2) Defendant Priddy fraudulently represented at an investor's conference in April, 1996 that ValuJet planned to add additional aircraft and that growth would be significant; and (3) Defendant Jordan fraudulently represented in a press release in April, 1996 that ValuJet's safety record had been certifiably among the very best in the airline industry. When viewing the allegations in the Complaint as true, the Court finds that Defendants Jordan and Priddy's alleged misrepresentations during the class period are sufficiently plead under the PSLRA heightened-pleading standards

---

[188] *See, e.g.*, *Bricklayers & Masons Local Union No. 5 Ohio Pension Fund v. Transocean Ltd.*, 866 F. Supp. 2d 223, 243 (S.D.N.Y. 2012) ("Likewise, the Complaint plausibly alleges facts indicating that a reasonable investor would assume that Transocean's safety and training measures were not only 'large in extent and range or amount,' but adequate, when, in fact, the measures were insufficient to address applicable legal requirements and created a high risk of legal exposure."); *In re Massey Energy Co. Sec. Litig.*, 883 F. Supp. 2d 597, 617-18 (S.D.W. Va. 2012) (holding that the defendants' statements concerning their commitment to safety, including that safety was a "first priority every day," were actionable); *In re ValuJet, Inc., Sec. Litig.*, 984 F. Supp. 1472, 1477-78 (N.D. Ga. 1997) (concluding that statements touting "operational integrity" and safety were false given numerous safety incidents).

> to constitute false statements for the purposes of a Rule 10b–5 claim.[189]

Similarly, the Defendants' representations that Equifax employed a highly sophisticated data information network are allegedly false given the actual state of its systems.

The case that the Defendants primarily rely upon, *In re Heartland Payment Systems, Inc. Securities Litigation* is distinguishable. In *Heartland*, the corporate defendant, a provider of bank card payment processing services to merchants, suffered a "Structured Query Language" attack by criminal hackers.[190] This attack placed hidden, malicious software on the defendant's network, which infected its payment processing system.[191] Because of this, hackers were able to steal 130 million credit card and debit card numbers.[192] After this incident, the plaintiffs filed a securities action, alleging that the defendants misrepresented the state of Heartland's network security, that they concealed the occurrence of data breach from investors, and they made false statements concerning the adequacy of its security systems and the efforts they took for network security.[193] Specifically, Heartland had stated that it "'place[d]

---

189 *ValuJet*, 984 F. Supp. at 1477-78.

190 *In re Heartland Payment Sys., Inc. Sec. Litig.*, Civ. No. 09-1043, 2009 WL 4798148, at *1 (D.N.J. Dec. 7, 2009).

191 *Id.*

192 *Id.*

193 *Id.* at *2.

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.'"[194] The plaintiffs argued that those statements were untruthful "because Heartland had suffered the SQL attack and had not fully resolved security issues arising out of that attack."[195] The court concluded, however, that these statements were not false or misleading because there was "nothing inconsistent" between these statements and "the fact that Heartland had suffered an SQL attack."[196] "The 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.'"[197] The court further explained that it was "equally plausible" that Heartland did place a high emphasis upon security.

In contrast, the Plaintiff here has not alleged that the Defendants' statements concerning Equifax's cybersecurity practices are false merely because Equifax suffered a security breach. Instead, the Plaintiff has asserted specific factual allegations describing the poor state of Equifax's cybersecurity. These allegations depict a data security system that was dangerously deficient and fell far short of industry standards. Unlike in *Heartland*, where it was

---

194 *Id.* at *5.

195 *Id.*

196 *Id.*

197 *Id.*

plausible that the company placed a high emphasis on security but nonetheless was a victim of a breach, Equifax's data security is alleged to have been in disrepair, in contrast to the Defendants' statements otherwise. Thus, *Heartland* is distinguishable.

The Defendants also argue that these allegations fail because the Plaintiff has failed to plead the falsity of the statements concerning the adequacy of cybersecurity with particularity.[198] The PSLRA requires a plaintiff to specify "the reason or reasons why the statement is misleading."[199] For example, the Defendants contend that the Plaintiff has not adequately alleged the falsity of the statement that the "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."[200] However, the Court concludes that the Plaintiff has satisfied its requirement to plead the falsity of these statements with particularity. The Plaintiff alleges in the Amended Complaint that this statement was false or misleading because Equifax "ignored advice issued by those external 'security experts' warning the Company about gross inadequacies in its cybersecurity," because Equifax "failed to heed the calls of its cybersecurity consultants to perform comprehensive

---

198 Defs.' Mot. to Dismiss, at 22.

199 15 U.S.C. § 78u–4(b)(1).

200 *See* Defs.' Mot. to Dismiss, at 22; *see also* Am. Compl. ¶ 292.

system reviews," and because Equifax's vulnerability scanning was deficient since scans were performed "infrequently, examined only portions of Equifax's systems, relied on outdated technology, and lacked appropriate redundancies."[201] The Defendants argue that these allegations merely second-guess the extent or efficacy of these efforts. However, the Court concludes that these allegations are sufficient because they explain why this statement was false, or at a minimum, misleading. These allegations explain that it was misleading to state that cybersecurity experts continually review Equifax's systems when Equifax ignored those experts' suggestions and used superficial vulnerability scanning.

The Defendants also challenge the statements that Equifax had a "rigorous enterprise risk management program" that targeted its cybersecurity risks,[202] that Equifax used "a variety of technical, administrative and physical ways to keep personal credit data safe,"[203] that Equifax "regularly review[ed] and update[d] [its] security protocols,"[204] and that Equifax "develop[ed], maintain[ed], and enhance[d] secured proprietary information databases."[205] According to the Defendants, the Plaintiff's allegations that Equifax's efforts were inadequate fail because they do not show that Equifax did not have a risk

---

201 Am. Compl. ¶ 293.

202 Am. Compl. ¶ 346.

203 *Id.* ¶ 339.

204 *Id.*

205 *Id.* ¶ 311.

management program, or that it did not attempt to comply with data security regulations.[206] However, the Plaintiff adequately alleges the falsity of each of these statements with particularity. With each of these statements, the Plaintiff explains how the context of Equifax's cybersecurity makes them false or misleading.[207] The Plaintiff alleges that each of these areas of cybersecurity was so deficient that it was misleading for Equifax to assure investors that these efforts were promoting the security of its data systems. These statements do more than merely tell investors that a risk management program existed or that it used various cybersecurity techniques. Instead, Equifax used these statements to assure investors that they were taking cybersecurity seriously.

Furthermore, the Defendants also take many of these statements out of context in their brief. For example, the Defendants argue that the Plaintiff has not shown that it was false or misleading to state that Equifax had an enterprise risk management program.[208] But, in the Amended Complaint, the Plaintiff alleges that Equifax stated that it has "a rigorous enterprise risk management program targeting . . . data security."[209] An assurance that Equifax employed a *rigorous* enterprise risk management program is more misleading

---

[206] Defs.' Mot. to Dismiss, at 22-23.

[207] *See* Am. Compl. ¶¶ 312, 340, 347 (explaining the falsity of each of these challenged statements).

[208] Defs.' Mot. to Dismiss, at 22.

[209] Am. Compl. ¶ 346.

to investors than simply affirming the existence of an enterprise risk management program. Similarly, the Defendants argue that the Plaintiff has not alleged that it was false to state that Equifax "regularly review[ed] and update[d] [its] security protocols," even if those efforts were not effective or to the necessary extent.[210] However, in the Amended Complaint, the Plaintiff alleges that Equifax stated that "[w]e regularly review and update our security protocols *to ensure that they continue to meet or exceed established best practices at all times.*"[211] This statement does not merely state that Equifax reviewed and updated its security protocols, but instead that it did so to *ensure* that it met established best practices. Furthermore, the Defendants argue that the Plaintiff has not shown that the statement that Equifax "monitor[ed] federal and state legislative and regulatory activities that involve credit reporting, data privacy and security" is false, when in reality the Plaintiff alleges that Equifax stated that "[w]e continuously monitor federal and state legislative and regulatory activities that involve credit reporting, data privacy and security to identify issues *in order to remain in compliance with all applicable laws and regulations*."[212] This context, omitted by the Defendants in their argument, is important in determining whether the statements were false or misleading.

---

[210] Defs.' Mot. to Dismiss, at 22.

[211] Am. Compl. ¶ 339 (emphasis added).

[212] *Compare* Defs.' Mot. to Dismiss, at 22-23, *with* Am. Compl. ¶ 342.

ii. Puffery

Next, the Defendants argue that many of the challenged statements concerning Equifax's commitment to data security constitute inactionable puffery.[213] Alleged misrepresentations must be based upon a material fact to give rise to a securities law violation.[214] "Subjective characterizations of a company's current performance or predictions about future performance, absent a false misstatement of fact, are generally not actionable."[215] Such statements of "corporate optimism" or "puffery" are not actionable because they both lack an underlying factual basis and also fail the materiality requirement of Rule 10b-5.[216] Thus, "vague, optimistic statements are not actionable because reasonable investors do not rely on them in making investment decisions."[217] Statements constitute "puffery" if they are "too general to cause a reasonable investor to rely upon them."[218] According to the Defendants, many of the alleged

---

[213] Defs.' Mot. to Dismiss, at 18-21.

[214] *Amalgamated Bank v. Coca-Cola Co.*, No. 1:05-CV-1226, 2006 WL 2818973, at *3 (N.D. Ga. Sept. 29, 2006).

[215] *Id.*

[216] *Id.*

[217] *Id.* (quoting *Grossman v. Novell, Inc.*, 120 F.3d 1112, 1119-20 (10th Cir. 1997)) (internal alterations omitted).

[218] *In re Australia & New Zealand Banking Grp. Ltd. Sec. Litig.*, No. 08 Civ. 11278(DLC), 2009 WL 4823923, at *11 (S.D.N.Y. Dec. 14, 2009) (quoting *ECA, Local 134 IBEW Joint Pension Tr. of Chi.*, 553 F.3d 187, 206 (2d Cir. 2009)).

statements reflected corporate optimism and aspiration that a reasonable investor would not rely upon, and thus constitute puffery. Such statements of puffery cannot serve as the basis for a section 10(b) claim because a reasonable investor would not rely upon them.[219] For example, the Defendants contend that many of the statements "generally avow a commitment to data security or characterize security as a priority for Equifax."[220] According to the Defendants, a reasonable investor would not rely upon statements such as these, which are "generalized, non-verifiable, and vague statements of commitment to and aspirations about data security."[221]

However, the Court finds that these alleged statements are not inactionable puffery. An alleged misstatement or omission must be "so obviously unimportant to a reasonable investor that reasonable minds could not differ on the question of their importance" to be deemed inactionable puffery.[222] For example, in the context of a drilling company's statements concerning its safety and training efforts, one court noted that it could not "say, as a matter of law, that Transocean's representation that such efforts were extensive was 'obviously unimportant' to GSF shareholders" since "[i]n an industry as dangerous as

---

219 Defs.' Mot. to Dismiss, at 18.

220 *Id.* at 19.

221 *Id.* at 18.

222 *Bricklayers & Masons Local Union No. 5 Ohio Pension Fund v. Transocean Ltd.*, 866 F. Supp. 2d 223, 239 (S.D.N.Y. 2012).

deepwater drilling, it is to be expected that investors will be greatly concerned about an operator's safety and training efforts."[223] Likewise, the Court cannot say, as a matter of law, that Equifax's representations that its cybersecurity efforts were extensive or that it was "committed" to data security were so "obviously unimportant" to its shareholders that they should be considered immaterial. Furthermore, the fact that these statements relate to a core aspect of Equifax's business makes it even more likely that a reasonable investor would assign weight to them. Since data security plays an important part of a business such as Equifax, investors would be even more likely to find these types of representations important in making their investment decisions. For these reasons, the Court cannot, as a matter of law, conclude that these statements are obviously unimportant to Equifax's investors.

Moreover, the context of these alleged statements is important to this determination. Although the alleged statements, when viewed in isolation, might constitute puffery, the fact that they were made repeatedly to assure investors that Equifax's systems were secure could lead a reasonable investor to rely upon them as reflecting the state of Equifax's cybersecurity.[224] Thus, the

---

[223] *Id.* at 244.

[224] *See In re Petrobras Sec. Litig.*, 116 F. Supp. 3d 368, 381 (S.D.N.Y. 2015) ("While some of the alleged statements, viewed in isolation, may be mere puffery, nonetheless, when (as here alleged) the statements were made repeatedly in an effort to reassure the investing public about the Company's integrity, a reasonable investor could rely on them as reflective of the true state of affairs at the Company. Accordingly, the Court cannot find that all of

context of these supposedly "aspirational" statements matters: the Defendants repeatedly stated that cybersecurity, an important aspect of their business, was a top priority for senior management, despite the fact that Equifax failed to employ some of the most elementary cybersecurity practices. Even if, in a vacuum, each of these statements seems like a meaningless, corporate vaguery, when taken together a reasonable investor would rely upon them to conclude that Equifax made cybersecurity a serious priority.

The cases cited by the Defendants are unpersuasive. For example, in *Ong v. Chipotle Mexican Grill, Inc.* (*Chipotle II*), the court concluded that statements that Chipotle was "committed to serving safe, high quality food" and that its "food safety programs are . . . designed to ensure" that Chipotle "compl[ies] with applicable federal, state and local food safety regulations" were inactionable puffery.[225] However, the court provided little analysis for why those statements constituted puffery. Here, statements affirming a commitment to cybersecurity can be actionable because a reasonable investor might rely upon such statements in making investment decisions. Although the court in *Chipotle II* found statements that the company was "committed" to serving safe food to constitute puffery, the Court concludes that the statements here are not so

---

Petrobras' alleged statements regarding its general integrity and ethical soundness were immaterial as a matter of law.").

[225] *Ong v. Chipotle Mexican Grill, Inc.* (*Chipotle II*), 294 F. Supp. 3d 199, 232 (S.D.N.Y. 2018).

obviously unimportant to investors given the repeated nature of these statements, the context of Equifax's business, and the widespread nature of the deficiencies alleged in the Amended Complaint. Therefore, for these reasons, *Chipotle II* is unpersuasive.

3. Failure to Disclose the Data Breach

Next, the Defendants move to dismiss the Plaintiff's allegations based upon their purported failure to disclose the Data Breach earlier.[226] In the Amended Complaint, the Plaintiff alleges that some of the alleged statements were or became misleading by omission because the Defendants did not publicly disclose the Data Breach until September 7, 2017.[227] According to the Plaintiff, the Defendants' statements after March 2017 lauding Equifax's data security were false or misleading because Equifax "knew or recklessly disregarded that hackers had already penetrated its databases."[228]

However, the Court concludes that the Defendants were under no duty to disclose the Data Breach prior to becoming aware of the incident in July 2017. The Plaintiff has not alleged that the Defendants knew about the Data Breach

---

[226] Defs.' Mot. to Dismiss, at 16.

[227] *See, e.g.*, Am. Compl. ¶ 318 (contending that certain statements, such as Equifax being a "trusted steward," were "false and misleading because Defendants knew or were reckless in failing to know, but failed to disclose, that hackers had penetrated Equifax's internal data systems"); *see also id.* ¶¶ 288, 300, 335, 338.

[228] Pl.'s Br. in Opp'n to Defs.' Mot. to Dismiss, at 28.

before July 29, 2017, but instead argues that they were reckless as to its occurrence. It bases its argument upon warnings that the Defendants allegedly received as to the deficient state of Equifax's cybersecurity, its failure to employ adequate patching processes, and its failure to use proper network monitoring. These warnings might demonstrate that the Defendants knew of, or were reckless as to, Equifax's ability to prevent or detect a breach. However, these warnings do not establish that the Defendants knew, or were reckless to the existence of, the specific Data Breach at issue here. The allegations also do not demonstrate that the Defendants knew of, or were reckless as to the existence of, Equifax's failure to patch the Apache Struts vulnerability. Therefore, the Defendants were under no duty to disclose the existence of the Data Breach before they knew it had occurred.

Second, the Plaintiff argues that the Defendants were under a duty to correct their prior misstatements once they became aware of the Data Breach in July 2017. According to the Plaintiff, even if some of the Defendants' statements may not have been misleading at the time they were made, the Defendants had a duty to correct the statements once they learned that the Data Breach had occurred.[229] A duty to disclose can be created by a defendant's previous decision to speak on the subject.[230] "Where a defendant's failure to

---

[229] Pl.'s Br. in Opp'n to Defs.' Mot. to Dismiss, at 29.

[230] *Rudolph v. Arthur Andersen & Co.*, 800 F.2d 1040, 1043 (11th Cir. 1986).

speak would render the defendant's own prior speech misleading or deceptive, a duty to disclose arises."[231] According to the Plaintiff, the Defendants had a duty to disclose once they learned that their prior statements concerning the security of Equifax's systems became false due to the Data Breach.[232]

However, the Court finds that the occurrence of the Data Breach did not itself make those prior statements false or misleading, and thus did not create a duty to disclose. As the Court noted above, the occurrence of a data breach does not necessarily imply that a company's data security is inadequate. In *Heartland*, the court concluded that the defendants were not under a duty to disclose the occurrence of a data breach because the plaintiffs had not alleged that the company's systems were actually deficient.[233] The court noted that the occurrence of a data breach itself does not establish that a company's data security is inadequate.[234] Similarly, here, the occurrence of the Data Breach itself did not necessarily render the Defendants' prior statements false, and thus

---

[231] *Id.* (citing *First Va. Bankshares v. Benson*, 559 F.2d 1307, 1314 (5th Cir. 1977)).

[232] Pl.'s Br. in Opp'n to Defs.' Mot. to Dismiss, at 29.

[233] *In re Heartland Payment Sys., Inc. Sec. Litig.*, Civ. No. 09-1043, 2009 WL 4798148, at *4 (D.N.J. Dec. 7, 2009).

[234] *Id.*

did not impose a duty to correct those statements by disclosing the occurrence of the Data Breach.[235] Therefore, the Court finds this argument unavailing.

4. Statements About Cybersecurity Risks

Next, the Defendants move to dismiss the Plaintiff's allegations regarding Equifax's warnings of its cybersecurity risks.[236] In the Amended Complaint, the Plaintiff alleges that Equifax, Smith, and Gamble made false or misleading statements in SEC filings concerning the cybersecurity risks that Equifax faced. The Plaintiff alleges that Equifax stated in its 2015 and 2016 Forms 10-K that:

> Despite our substantial investment in physical and technological security measures, employee training, contractual precautions and business continuity plans, our information technology networks and infrastructure or those of our third-party vendors and other service providers could be vulnerable to damage, disruptions, shutdowns, or breaches of confidential information due to criminal conduct, denial of service or other advanced persistent attacks by hackers[.][237]

However, according to the Plaintiff, it was false or misleading to state that Equifax "*could* be vulnerable" to a breach "when, in fact, Equifax *was* highly

---

[235] However, as discussed above, the Plaintiff has adequately alleged that those prior statements were false. Whether those statements touting Equifax's cybersecurity are false, and thus actionable, is a separate question from whether the Defendants were under a duty to disclose specifically the occurrence of the Data Breach. Those statements are actionable merely because of the fact that they *were* false or misleading at the time they were made due to the widespread inadequacies in Equifax's data systems, notwithstanding whether the Data Breach occurred or not.

[236] Defs.' Mot. to Dismiss, at 26.

[237] Am. Compl. ¶ 306.

vulnerable to such an attack, as, in fact, Defendants had been warned on numerous occasions both before and during the Class Period."[238]

The Defendants argue that these allegations fail to state a claim because, through these statements, the Defendants warned of the precise risk that caused the Plaintiff's losses.[239] The Court finds that these statements are not actionable. The difference between disclosing that Equifax "could be vulnerable" and that it was "highly vulnerable" would not mislead a reasonable investor in making an investment decision. The case that the Plaintiff relies upon, *In re Van der Moolen Holding N.V. Securities Litigation*, is distinguishable.[240] There, the court concluded that cautionary statements can give rise to a section 10(b) violation.[241] The court noted that "to caution that it is only possible for the unfavorable events to happen when they have already occurred is deceit."[242] However, that case is distinguishable. There, the defendant warned investors about regulatory risks, even though it knew or was recklessly ignorant that its employees were violating NYSE rules.[243] Here, in contrast, the risk warned of

---

238 *Id.* ¶ 308 (emphasis in original).

239 Defs.' Mot. to Dismiss, at 27.

240 *In re Van der Moolen Holding N.V. Sec. Litig.*, 405 F. Supp. 2d 388 (S.D.N.Y. 2005).

241 *Id.* at 400.

242 *Id.* (internal quotations omitted).

243 *Id.*

is different. The Defendants warned that Equifax could be vulnerable to a data breach, but they did not fail to disclose the existence of a breach when they made that statement. Thus, unlike in *Van der Moolen*, the Defendants did not warn that Equifax could be at risk, when it in fact was suffering a data breach. Therefore, the Court finds these risk statements inactionable.

5. Equifax's Compliance With Data Protection Laws

Next, the Defendants move to dismiss the Plaintiff's claims concerning statements about Equifax's compliance with data protection laws, regulations, and best practices. In the Amended Complaint, the Plaintiff alleges that the Defendants made various statements assuring that Equifax complied with relevant data protection laws, regulations, standards, and best practices. For example, the Plaintiff alleges that Equifax stated on its website that it "takes great care to ensure that we use and process personal data in ways that comply with applicable regulations and respects individual privacy."[244] Equifax also stated that "[w]e regularly review and update our security protocols to ensure that they continue to meet or exceed established best practices at all times"[245] and that "[w]e continuously monitor federal and state legislative and regulatory activities that involve credit reporting, data privacy and security to identify issues in order to remain in compliance with all applicable laws and

---

[244] Am. Compl. ¶ 336.

[245] *Id.* ¶ 339.

regulations."[246] However, despite these affirmations, Equifax allegedly fell far short of complying with these regulatory requirements.

The Defendants first assert that these claims merely allege corporate mismanagement, which is not actionable under federal securities laws.[247] However, as explained above, this argument fails. The Plaintiff does not allege that the Defendants violated section 10(b) by failing to comply with cybersecurity laws, regulations, and best practices. Instead, the Plaintiff argues that they violated section 10(b) by stating that Equifax was in compliance with these laws and regulations, when in fact it was not. As stated above, the Court finds that such a claim is actionable under federal securities laws. If the Plaintiff adequately alleged that Equifax made false statements concerning its compliance with these laws, regulations, and standards, then such claims would not be barred by *Santa Fe*.

The Defendants next argue that these alleged statements described Equifax's ongoing *efforts* to comply with data protection laws and standards, and that the statements did not guarantee compliance.[248] According to the Defendants, the Plaintiff has not adequately alleged the falsity of these statements because the fact that they were not in compliance does not mean

---

246 *Id.* ¶ 342.

247 Defs.' Mot. to Dismiss, at 21.

248 Defs.' Reply Br., at 23.

that they were not making efforts to comply. However, in the alleged statements, Equifax did more than just say that it made efforts to comply with these laws and standards. It stated that it monitored regulatory activities to "*remain in compliance* with all applicable laws and regulations," that it reviewed its security protocols to "ensure that they continue to meet or exceed established best practices," and that it took "great care" to ensure that it handled personal data in a way that complied with regulations.[249] These statements go beyond merely stating that it made an effort to comply with laws, regulations, and industry standards, and instead assured that Equifax took steps to remain in compliance with laws and regulations and meet industry standards. According to the allegations in the Amended Complaint, Equifax in reality failed to live up to these assurances.

And even if these statements only conveyed that Equifax made an effort to comply with data security laws, regulations, and standards, they would still be false or misleading. A reasonable investor would understand these statements to assure that the company was making actual, good faith efforts to maintain a data security protocol that complied with these standards. In reality, according to the Amended Complaint, data security was not a priority at all for Equifax's management.[250] The state of Equifax's cybersecurity reflected a

---

[249] Am. Compl. ¶¶ 340, 342.

[250] *See, e.g.*, Am. Compl. ¶¶ 66-67.

"systemic organizational disregard for cybersecurity."[251] Given this context, these statements were false or misleading. It is misleading to a reasonable investor to state that Equifax made an effort to comply with data laws, regulations, and standards when, in fact, Equifax demonstrated a systemic disregard for cybersecurity. For this reason, these statements concerning efforts to comply with data laws, regulations, and industry best practices are false or misleading.

The Defendants also argue that the fact Equifax experienced a cyberattack does not render their aspirational statements concerning their data security efforts and compliance false.[252] However, as the Court explained with regard to the statements concerning the adequacy of Equifax's cybersecurity, the Plaintiff does not rely solely upon the occurrence of the Data Breach to show the falsity of the compliance statements. Instead, the Plaintiff alleges that these statements regarding Equifax's compliance with data security laws, regulations, and standards were false due to widespread deficiencies in Equifax's cybersecurity and data protocols. According to the Plaintiff, Equifax assured the public that it made efforts to remain in compliance with data laws, regulation, and standards, even though in reality its cybersecurity was in a state of disrepair. Therefore, under the facts alleged, these assurances that Equifax

---

[251] *Id.* ¶ 66.

[252] Defs.' Mot. to Dismiss, at 17.

made efforts to comply with data protection laws and best practices were false or misleading.

Next, the Defendants also argue that these allegations fail because, unlike in the cases relied upon by the Plaintiff, the Plaintiff's allegations do not show that the Defendants had contemporaneous knowledge of the facts contradicting their statements concerning legal compliance.[253] However, this argument addresses whether the Defendants acted with the requisite scienter, which is addressed below. Whether a statement is false or misleading, and whether a defendant made such a statement with the requisite state of mind, are two separate questions. As discussed above, the Plaintiff has adequately alleged that these statements were false or misleading.

Finally, at oral argument, the Defendants distinguished the cases relied upon by the Plaintiff. They contended that the defendants' statements in those cases concerning their compliance with regulations were false because they had already been told by regulators that their operations were deficient.[254] It is true that, in some of those cases, the court found the defendants' statements misleading due in part to the fact that regulators had informed them of problems in their operations.[255] However, this does not mean that any statement

---

253 Defs.' Reply Br., at 24.

254 Transcript of Oral Argument, at 75 [Doc. 83].

255 *See, e.g.*, *In re Cryolife, Inc.*, No. Civ.A.1:02CV1868-BBM, 2003 WL 24015055, at *8-*9 (N.D. Ga. May 27, 2003) (noting that the defendant had

touting compliance with laws, regulations, or industry standards is not false or misleading if the company has not received communications from regulators. Instead, this was just one fact that supported the courts' holdings in those cases. Here, the Defendants issued statements assuring that Equifax remained in compliance with data security laws, regulations, and standards, even though its security systems were grossly deficient. As described above, these statements were false or misleading to investors, even if Equifax had never received an enforcement letter from regulators informing it that it was not in compliance with data laws or regulations.

6. Statements Concerning Internal Controls

The Defendants next move to dismiss the Plaintiff's allegations concerning the Defendants' various statements about Equifax's internal controls. In the Amended Complaint, the Plaintiff alleges that Smith and Gamble certified in SEC filings, pursuant to the Sarbanes-Oxley Act, that

---

contended it was in compliance with all FDA regulations despite the fact that it had "received a letter from the FDA documenting specific problems with Cryolife's quality assurance programs"); *In re ValuJuet, Inc.*, 984 F. Supp. 1472, 1477 (N.D. Ga. 1997) ("In the Complaint, the Plaintiffs allege that representatives of the Federal Aviation Administration ('FAA') identified numerous safety-related incidents involving ValuJet. The Plaintiffs further allege in the Complaint that in February of 1996, the FAA (1) began surveillance of ValuJet; (2) expressed written concern about the training of pilots and ValuJet's safety and maintenance procedures which included numerous, uncorrected violations; and (3) as a result of the February 1996 inspection, expressly required ValuJet to get FAA approval before buying more planes or beginning access to new cities. As alleged in the Complaint, an FAA letter to Defendant Jordan, dated February 29, 1996, expressed concern about ValuJet's meeting the highest possible degree of safety in the public interest.").

Equifax maintained a system of internal controls that would 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."[256] Nonetheless, according to the Plaintiff, these assurances in Equifax's 10-K and 10-Q filings concerning the quality of its internal controls were materially false or misleading because Equifax lacked adequate mechanisms for detecting and responding to data breaches.[257] The Defendants move to dismiss the allegations concerning this category of statements. They argue that the Plaintiff has failed to plead the falsity of the challenged statements because they address Equifax's internal controls over *financial reporting*, as opposed to controls over data security.[258] According to the Defendants, since these statements exclusively addressed financial reporting controls at Equifax, deficiencies in Equifax's cybersecurity mechanisms do not render these statements false.[259] Thus, deficiencies in Equifax's data breach protocol do not establish that these statements were false.

The Court concludes that the Plaintiff has failed to show that these statements are false. "Congress enacted Sarbanes-Oxley to restore investor confidence in the wake of numerous, highly-publicized, cases of accounting

---

256 Am. Compl. ¶ 349.

257 *Id.* ¶¶ 349-53.

258 Defs.' Mot. to Dismiss, at 30-31.

259 *Id.* at 31-32.

fraud."[260] The purpose of Sarbanes-Oxley certifications is to ensure that proper financial reporting processes are undertaken. In *In re PetroChina Co. Ltd. Securities Litigation*, the district court rejected a section 10(b) claim premised upon PetroChina's Sarbanes-Oxley certifications.[261] The court noted that the plaintiffs' allegations, concerning bribery by PetroChina officials, did not "imply that the Company had flawed internal controls over *financial reporting.*"[262] The court explained that the plaintiffs did "not claim that PetroChina failed to evaluate its internal controls or disclose any weaknesses to its auditors," did not "assert that the certifying officers neglected to inform PetroChina's auditor of any relevant fraud," and did not "establish that PetroChina's internal controls in relation to *financial reporting* were insufficient; much less does the [complaint] make any allegation as to how or why PetroChina's internal controls were inadequate."[263]

Likewise, the Plaintiff fails to allege that Equifax had flawed internal controls over its financial reporting. Even if Equifax's data breach protocol was vastly deficient, this does not establish that it had insufficient internal controls over financial reporting. The Plaintiff has not raised any allegations concerning

---

[260] *City of Roseville Emp. Ret. Sys. v. Horizon Lines, Inc.*, 686 F. Supp. 2d 404, 417 (D. Del. 2009).

[261] *In re PetroChina Co. Ltd. Sec. Litig.*, 120 F. Supp. 3d 340, 358-59 (S.D.N.Y. 2015).

[262] *Id.* at 359.

[263] *Id.*

the accuracy of Equifax's accounting, books, or financial reporting. Therefore, the Plaintiff has not established that Equifax, Smith, or Gamble's statements concerning Equifax's internal controls over financial reporting were false. A reasonable investor would understand that certifications under Sarbanes-Oxley such as these are in the context of financial accounting scandals, and would recognize that it related to Equifax's financial reporting. A reasonable investor would not take assurances of internal controls to detect improprieties in accounting and bookkeeping to guarantee that there were systems in place to deal with cybersecurity breaches. Since the Plaintiff has not alleged that Equifax's financial reports were inaccurate in any way, its claims concerning Smith and Gamble's certification of proper internal controls pursuant to Sarbanes-Oxley fail.[264] Therefore, the Plaintiff's claims are dismissed to the extent that they rely upon statements guaranteeing adequate internal controls pursuant to Sarbanes-Oxley.

7. Statements of Opinion and Belief

Next, the Defendants contend that many of the challenged statements are inactionable opinions or statements of belief.[265] First, the Defendants contend that almost all of the alleged statements are inactionable, in part, because they

---

[264] *See In re Braskem S.A. Sec. Litig.*, 246 F. Supp. 3d 731, 758 (S.D.N.Y. 2017) (rejecting securities fraud claims premised upon Sarbanes-Oxley certifications because the complaint did not "concretely allege that any of Braskem's financial reports were in any way inaccurate").

[265] Defs.' Mot. to Dismiss, at 24-26.

are opinions.[266] However, many of these statements that the Defendants contend are inactionable are not, in fact, opinions. For example, the Defendants contend that the following statement is an inactionable opinion: "As a trusted steward of consumer and business information, Equifax employs strong data security and confidentiality standards on the data we provide and on the access to that data. We maintain a highly sophisticated data information network that includes advanced security, protections and redundancies."[267] While such statements use some indefinite language, they do not constitute a subjective opinion.

However, some of the allegedly false statements are closer calls. According to the Defendants, statements such as Smith's assurance that "I think we are in a very good position now" are not actionable because the Plaintiff has not shown that the Defendants did not in fact hold the stated opinions.[268] The Plaintiff contends that this statement, even if an opinion, is actionable because it did not align with the information in his possession.[269] "[C]ertain opinions may be actionable because 'if the real facts are otherwise, but not provided, the

---

266 *See generally* [Doc. 62-2].

267 *See* [Doc. 62-2], at 2.

268 Defs.' Mot. to Dismiss, at 24-25.

269 Pl.'s Br. in Opp'n to Defs.' Mot. to Dismiss, at 38.

opinion statement will mislead its audience.'"[270] An investor "expects not just that the issuer believes the opinion (however irrationally), but that it fairly aligns with the information in the issuer's possession at the time."[271] Opinion statements can be "misleading in context," and thus "actionable," if they "conflict with what a reasonable investor would take from the statement itself."[272]

As discussed in more detail below, the Plaintiff only alleges that Smith – not the other Individual Defendants – was given specific information as to the deficiencies in Equifax's cybersecurity. Around March 2017, Smith oversaw Mandiant's audit of Equifax's systems, where Mandiant warned that these systems were inadequate. The Plaintiff has not made specific allegations that Gamble, Ploder, or Dodge had information in their possession contradicting any opinion statements they issued. Without this knowledge, these opinion statements are not actionable. Furthermore, any opinion statements Smith made before receiving these warnings would also not be actionable.

B. Scienter

Next, the Defendants argue that the Plaintiff has failed to plead facts that give rise to a strong inference of scienter on the part of any of the Defendants.

---

[270] *In re Flowers Foods, Inc. Sec. Litig.*, No. 7:16-CV-222 (WLS), 2018 WL 1558558, at *8 (M.D. Ga. Mar. 23, 2018) (quoting *Omnicare, Inc. v. Laborers Dist. Council Constr. Indus. Pension Fund.*, 135 S. Ct. 1318, 1328 (2015)).

[271] *Omnicare*, 135 S. Ct. at 1329.

[272] *Flowers Foods*, 2018 WL 1558558, at *8 (quoting *Omnicare*, 135 S. Ct. at 1329).

To state a section 10(b) claim, the PSLRA requires a plaintiff "to plead with particularity facts giving rise to a strong inference that the defendants either intended to defraud investors or were severely reckless when they made the allegedly materially false or incomplete statements."[273] A "strong inference" is an inference that is "cogent and at least as compelling as any opposing inference one could draw from the facts alleged."[274] This inquiry asks whether all of the facts alleged, taken as a whole, give rise to this strong inference of scienter.[275] Thus, courts must consider the complaint in its entirety, and "not whether any individual allegation, scrutinized in isolation, meets that standard."[276] This inquiry is "inherently comparative" because courts must take into account plausible opposing inferences.[277] Where a lawsuit involves multiple defendants and multiple allegations, moreover, "scienter must be found with respect to each defendant and with respect to each alleged violation of the statute."[278]

---

[273] *Mizzaro v. Home Depot, Inc.*, 544 F.3d 1230, 1238 (11th Cir. 2008) (internal quotations omitted).

[274] *Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 324 (2007).

[275] *Mizzaro*, 544 F.3d at 1238.

[276] *Id.* at 1238.

[277] *Id.* at 1239 (quoting *Tellabs*, 551 U.S. at 323).

[278] *Phillips v. Scientific-Atlanta, Inc.*, 374 F.3d 1015, 1017 (11th Cir. 2004).

To move beyond the pleading state, a plaintiff "must allege facts sufficiently demonstrating each defendant's state of mind regarding his or her alleged violations."[279] But, the PSLRA does permit the aggregation of facts to infer scienter.[280] The factual allegations, taken as a whole, must give rise to this strong inference as to each Defendant and each alleged violation.[281] Circumstantial evidence can be sufficient to establish a strong inference of scienter.[282] Since scienter is highly fact-intensive inquiry, such questions are most appropriate for a fact finder.[283] "In sum, the reviewing court must ask: When the allegations are accepted as true and taken collectively, would a reasonable person deem the inference of scienter at least as strong as any opposing inference?"[284]

In the Eleventh Circuit, it is well established that section 10(b) and Rule 10b-5 require a showing of either an intent to deceive, manipulate, or defraud,

---

[279] *Id.* at 1018.

[280] *Id.* at 1017; *see also In re Cabletron Sys., Inc.*, 311 F.3d 11, 39 (1st Cir. 2002) ("The plaintiff may combine various facts and circumstances indicating fraudulent intent—including those demonstrating motive and opportunity—to satisfy the scienter requirement." (internal alterations and quotations omitted)).

[281] *Phillips*, 374 F.3d at 1018.

[282] *Mizzaro*, 544 F.3d at 1249.

[283] *In re Sci. Atlanta, Inc. Sec. Litig.*, 754 F. Supp. 2d 1339, 1361 (N.D. Ga. 2010) (citing *S.E.C. v. Merchant Capital, LLC*, 483 F.3d 747, 766 (11th Cir. 2007)).

[284] *Tellabs*, 551 U.S. at 326.

or severe recklessness.[285] The Eleventh Circuit has defined "severe recklessness" as:

> Severe recklessness is limited to those highly unreasonable omissions or misrepresentations that involve not merely simple or even inexcusable negligence, but an extreme departure from the standards of ordinary care, and that 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.[286]

"Plaintiffs may prove such recklessness by providing evidence that defendants possessed knowledge of facts or access to information contradicting their public statements, so as to prove that defendants knew or should have known that they were misrepresenting material facts related to the corporation."[287] "Facts indicating the scienter may include the particular times, dates, places, or other details of the alleged fraudulent activity."[288] These particulars "are not required per se," but "their absence from the complaint may be indicative of the excessive generality of the allegations' supporting scienter."[289] "With regard to Individual Defendants, the question is 'whether a reasonable person would infer that there

---

[285] *Mizzaro*, 544 F.3d at 1238.

[286] *Id.* (quoting *Bryant v. Avado Brands, Inc.*, 187 F.3d 1271, 1282 n.18 (11th Cir. 1999)).

[287] *In re Sci. Atlanta, Inc. Sec. Litig.*, 754 F. Supp. 2d 1339, 1360 (N.D. Ga. 2010) (citing *Cornwell v. Credit Suisse Grp.*, 689 F. Supp. 2d 629, 637 (S.D.N.Y. 2010)).

[288] *In re Coca-Cola Enters. Inc. Sec. Litig.*, 510 F. Supp. 2d 1187, 1199 (N.D. Ga. 2007).

[289] *Id.* (internal quotations omitted).

was at least a fifty-fifty chance that the individual defendants knew about the alleged fraud (or were severely reckless in not knowing about it) based on its nature, duration, or amount.'"[290]

Here, the Plaintiff attempts to plead scienter by alleging, among other things, that: (1) the Defendants received numerous warnings concerning the inadequacies of Equifax's cybersecurity; (2) the Defendants were aware of the breach by late July 2017, but failed to disclose the breach and continued to make false statements until September 7, 2017; (3) the false and misleading statements concerned one of the most significant issues and severe risks that Equifax faced; (4) the Defendants were in charge of cybersecurity and received routine updates about the state of Equifax's data security; (5) the egregiousness of the deficiencies in Equifax's data security practices supports an inference of scienter; (6) the sudden departure of high-ranking officers at Equifax after disclosure of the Data Breach supports a finding of scienter; and (7) suspicious stock sales by Gamble and Ploder support an inference of scienter.[291] Since scienter is an essential element of a securities fraud claim, the Plaintiff must create a strong inference – one that is "cogent and compelling" – that the Defendants knew about the deficiencies in Equifax's cybersecurity, or were severely reckless in not knowing about it, when they made the allegedly false or

---

[290] *In re Ebix, Inc. Sec. Litig.*, 898 F. Supp. 2d 1325, 1344 (N.D. Ga. 2012) (quoting *Mizzaro*, 544 F.3d at 1249)).

[291] Am. Compl. ¶¶ 267-84.

misleading statements.[292] The Court concludes that the allegations in the Amended Complaint establish a strong inference of scienter as to Equifax and Smith. However, these facts, even when taken together, do not give rise to a strong inference of scienter as to Gamble, Dodge, and Ploder.

1. Warnings About Data Security Deficiencies

First, the Defendants argues that alleged warnings of deficiencies in Equifax's cybersecurity fail to support a strong inference of scienter as to any of the Individual Defendants.[293] In the Amended Complaint, the Plaintiff alleges that the "Defendants received numerous warnings . . . that Equifax's cybersecurity was inadequate to protect the sensitive personal information in its custody" and that this contributes to a finding of scienter.[294] Specifically, the Plaintiff alleges that: (1) Deloitte and KPMG issued audit reports detailing several problems with Equifax's cybersecurity, but Equifax's management did not take these reports seriously;[295] (2) Smith oversaw a March 2017 investigation by security consulting firm Mandiant, in which Mandiant warned that Equifax's cybersecurity was inadequate and contained critical weaknesses;[296] (3) security researchers warned Equifax that cybersecurity

---

292 *Mizzaro*, 544 F.3d at 1247.

293 Defs.' Mot. to Dismiss, at 35.

294 Am. Compl. ¶ 268.

295 *Id.* ¶¶ 71, 269.

296 *Id.* ¶ 268.

deficiencies existed, including an "immense cache of personal consumer information" that was accessible through public-facing websites;[297] (4) Equifax received clear warnings about the Apache Struts vulnerability from both the government and its own employees;[298] (5) Equifax employees warned "management" that the company's cybersecurity was inadequate, but data security was not a priority for management;[299] and (6) Equifax prior breaches that revealed cybersecurity vulnerabilities to the Defendants.[300] According to the Defendants, these allegations do not give rise to a strong inference of scienter because the Plaintiff has failed to plead facts showing that these supposed warnings were ever communicated to any of the Individual Defendants.[301]

The Court finds that these allegations provide sufficient circumstantial evidence to conclude that Smith was aware of the warnings concerning the deficiencies in Equifax's cybersecurity. In the Amended Complaint, the Plaintiff alleges that Equifax hired Mandiant in early 2017 to conduct a cybersecurity audit after the W2Express breach in 2016.[302] Specifically, the Plaintiff alleges that "Equifax hired cybersecurity firm Mandiant to investigate weaknesses in

---

297 *Id.* ¶ 269.

298 *Id.* ¶ 271.

299 *Id.*

300 *Id.* ¶ 270.

301 Defs.' Mot. to Dismiss, at 35-36.

302 Am. Compl. ¶ 13.

its data protection systems" and that "Smith was personally overseeing, and closely monitoring the progress of, this investigation."[303] This allegation is based upon a *Bloomberg* report published in the wake of the Data Breach. The Plaintiff alleges that Mandiant "warned Equifax that its unpatched systems and misconfigured security policies could indicate major problems."[304] However, instead of heeding Mandiant's advice, Equifax allegedly disputed the firm's findings and declined to engage in a broader review of Equifax's data security.[305] Based upon this, the Court concludes that the Plaintiff adequately alleges that Smith knew, or was severely reckless as to the existence of, warnings of serious deficiencies in Equifax's cybersecurity after receiving Mandiant's warnings in early 2017.

The Defendants then argue that these allegations should not be given weight because they are based upon articles in *Bloomberg* and *Motherboard* that rely upon anonymous sources.[306] In *Mizzaro*, the Eleventh Circuit addressed the question of how to weigh allegations based upon confidential witness reports.[307]

---

303 *Id.* ¶ 91 (emphasis omitted).

304 *Id.* ¶ 92.

305 *Id.* ¶ 93.

306 Defs.' Mot. to Dismiss, at 36-37.

307 *See Mizzaro*, 544 F.3d at 1239 ("One topic *Tellabs* did not address is how courts should go about evaluating allegations based on statements made by unidentified, confidential witnesses. The issue is important here because statements by confidential witnesses form one of the main building blocks of the amended complaint.").

There, the court noted that "[a]lthough a whistleblower who demands confidentiality may be less credible than one who is willing to put his name behind his accusations," allegations based on such statements are not "heavily discounted" in all cases.[308] It explained that "the weight to be afforded to allegations based on statements proffered by a confidential source depends on the particularity of the allegations made in each case, and confidentiality is one factor that courts may consider."[309] "Confidentiality, however, should not eviscerate the weight given if the complaint otherwise fully describes 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."[310]

In the Amended Complaint, the Plaintiff bases some of its allegations upon news articles citing anonymous sources. For example, the Plaintiff bases some of its allegations on a *Bloomberg* article reported on September 29, 2017.[311] That article explained that the Mandiant investigation was "described internally as 'a top-secret project' and one that Smith was overseeing personally, according to one person with direct knowledge of the matter."[312] The Plaintiff also

---

308 *Id.* at 1239.

309 *Id.* at 1240.

310 *Id.*

311 Am. Compl. ¶¶ 91-93.

312 *Id.* ¶ 91 (emphasis omitted).

premised some of its allegations upon an article published in *Motherboard* on October 26, 2017. Despite the fact that these news articles rely in part on anonymous sources, the Court declines to completely discount the allegations that rely upon them. This Court has previously noted that pleading requirements under the PSLRA can easily be satisfied with references to "internal memoranda" and "news articles."[313] News articles, which frequently rely upon unnamed sources, constitute reliable bases for allegations. Therefore, the Court does not discount the allegations based upon these two articles merely because they cite anonymous sources. And, even if the Plaintiff did in fact rely solely upon information derived from an anonymous source, and not information from a news article, these allegations would still be entitled to weight. The *Bloomberg* article cites two independent sources, with direct knowledge, who corroborate each other's assertions.[314] Furthermore, the *Motherboard* article provides statements from several former Equifax employees, providing both their positions and tenure in the company.[315] The Court therefore finds that the allegations based upon these news articles are entitled to due consideration.

---

[313] *In re Theragenics Corp. Sec. Litig.*, 105 F. Supp. 2d 1342, 1355 (N.D. Ga. 2000).

[314] Am. Compl. ¶¶ 91-94.

[315] *See, e.g.*, *id.* ¶ 77 ("Regarding those warnings, in an October 26, 2017 article entitled 'Equifax Was Warned,' *Motherboard* reported that according to a former member of Equifax's cybersecurity team who left the Company in 2017, the Company had hired Deloitte to perform a security audit in 2016."); *see also id.* ¶¶ 78, 80-83.

However, the Plaintiff's allegations of scienter fail as to the rest of the Individual Defendants. The Plaintiff has not provided sufficiently "particularized averments of fraud or scienter" as to Gamble, Ploder, and Dodge to give rise to a strong inference that they acted with knowledge or severe recklessness.[316] "Claims of securities fraud cannot rest on speculation and conclusory allegations."[317] The Plaintiff has not adequately pleaded that Gamble, Ploder or Dodge ever received any of these purported warnings as to the shortcomings in Equifax's data security. Instead, the Plaintiff relies upon general allegations that Equifax "management" was warned but did not heed experts' advice.[318] Such generalities do not establish a strong inference of scienter. The Plaintiff has not alleged "which defendant knew what, how they knew it, or when" with regard to these warnings.[319]

---

[316] *Garfield v. NDC Health Corp.*, 466 F.3d 1255, 1265 (11th Cir. 2006).

[317] *Id.* (internal quotations omitted).

[318] *See, e.g.*, Am. Compl. ¶ 254 ("For example, as alleged above, a former Equifax employee told Motherboard that Company management refused to take seriously the conclusions of a 2016 Deloitte security audit that found multiple serious deficiencies in the Company's infrastructure, including poor patching.").

[319] *In re Theragenics Corp. Sec. Litig.*, 105 F. Supp. 2d 1342, 1361 (N.D. Ga. 2000) (quoting *In re Comshare, Inc. Sec. Litig.*, No. 96-737-DT, 1997 WL 1091468, at *8 (E.D. Mich. Sept. 18, 1997)).

The Plaintiff relies upon *In re ChoicePoint, Inc. Securities Litigation*[320] to support its argument that these allegations sufficiently plead scienter.[321] However, that case is distinguishable. In *ChoicePoint*, the plaintiffs alleged that the defendants misrepresented the existence and severity of data security problems within the company prior to a data breach.[322] The court concluded that the plaintiffs adequately alleged scienter. Specifically, the plaintiffs alleged that the individual defendants "had access to internal information demonstrating the falsity of the public statements and were confronted by employees," that employees specifically warned each of the individual defendants about the company's inadequate security procedures, and that some of the individual defendants learned of the company's data breach and subsequently sold millions of dollars of their company stock. In contrast, the Plaintiff has not alleged that Gamble, Dodge, and Ploder were specifically warned about the problems with Equifax's data security, and did not specifically allege that each of these defendants had access to information contradicting their public statements. Instead, the Plaintiff relies on general allegations that "management" was warned. Such an allegation requires the Court to assume that Gamble, Dodge,

---

320 *In re ChoicePoint, Inc. Sec. Litig.*, No. 1:05-CV-00686-JTC, 2006 WL 8429145 (N.D. Ga. Nov. 21, 2006).

321 Pl.'s Br. in Opp'n to Defs.' Mot. to Dismiss, at 41.

322 *In re ChoicePoint,* at *1-2.

and Ploder were part of this group of "management" that received these warnings. This assumption does not give rise to a strong inference of scienter.

The Plaintiff also argues that this stringent requirement for scienter ignores recklessness as a way to establish scienter. According to the Plaintiff, it is not required to provide "smoking gun" evidence of scienter, but instead can establish recklessness through the Individual Defendants' "access to a plethora of information clearly and directly contradicting their public statements regarding cybersecurity."[323] While it is true that the Plaintiff need not provide a "smoking gun" of scienter, it also cannot rely on generalities and chains of inferences. The Plaintiff must allege specific facts as to each defendant and each challenged statement that give rise to a strong inference of scienter. To establish a strong inference of recklessness, the Plaintiff must allege facts showing that the risk of misleading investors was so obvious that the Defendants must have been aware of it. The Plaintiff's allegations fail to meet this standard.

The Defendants also argue that, even if these warnings and concerns had been communicated to the Individual Defendants, the Plaintiff fails to plead facts establishing that they agreed with any of these concerns or were severely reckless in not believing them.[324] Thus, with regard to Smith, even though he personally oversaw the Mandiant audit, the Plaintiff does not allege that he

---

[323] Pl.'s Br. in Opp'n to Defs.' Mot. to Dismiss, at 42.

[324] Defs.' Mot. to Dismiss, at 38-39.

agreed with the firm's conclusion that Equifax's cybersecurity was deficient. However, the Plaintiff need not allege that Smith agreed subjectively with Mandiant's concerns to establish scienter. In *Omnicare*, the Supreme Court explained that an issuer's statement that its conduct is lawful, when made contrary to its lawyers' advice, can give rise to a section 10(b) claim.[325] Similarly, Smith's statements touting Equifax's cybersecurity, despite his knowledge of experts' advice to the contrary, are actionable.

Next, the Defendants argue that the prior data breaches fail to establish a strong inference of scienter because they did not put them on notice of inadequacies in Equifax's systems.[326] In the Amended Complaint, the Plaintiff alleges that the prior W2Express, LifeLock, and TALX breaches warned the Defendants that Equifax's cybersecurity was vulnerable.[327] Thus, according to the Plaintiff, the Defendants knew or were severely reckless as to the deficient state of Equifax's cyberdefenses. According to the Defendants, the Plaintiff has not pleaded facts showing that these prior incidents were symptomatic of broader cybersecurity problems, and thus cannot be used to show that the Defendants were aware of the deficiencies in the data systems. The Defendants argue that these breaches did not put them on warning because none of them

---

[325] *Omnicare, Inc. v. Laborers Dis. Council Const. Indus. Pension Fund.*, 135 S. Ct. 1318, 1328-29 (2015).

[326] Defs.' Mot. to Dismiss, at 39-40.

[327] Am. Compl. ¶¶ 73-75, 84-90.

"remotely resemble[d]" the attack in the Data Breach.[328] According to the Defendants, these prior breaches did not involve the same exact exploitation of unpatched software vulnerabilities.

The Court agrees with the Plaintiff that these prior breaches were symptomatic of a larger cybersecurity problem. The Amended Complaint details how these prior incidents were the result of many of the same problems that contributed to the Data Breach here. According to the Amended Complaint, these previous breaches resulted from, or were exacerbated by, poor authentication measures and inadequate network monitoring.[329] In fact, after one of these incidents, Equifax acknowledged that it would need to implement additional monitoring and blocking measures to protect the data in its

---

[328] Defs.' Reply Br., at 1-2.

[329] *See* Am. Compl. ¶ 69 ("The hackers gained unauthorized access to data on Equifax's computer systems by using publicly available information to answer security questions and bypass authentication measures."); *id.* ¶ 70 ("Because Equifax failed to implement adequate network monitoring safeguards, hackers were able to repeatedly penetrate Equifax's network for approximately eight months before the Company finally detected the 'suspicious inquiries' in January 2014."); *id.* ¶¶ 73-74 ("Once again, Equifax's inadequate network monitoring practices compounded the magnitude of its failure to implement proper authentication protocols: the W2Express hackers first penetrated the Company's networks in early 2015 and remained undetected inside Equifax's networks for approximately one year before they were discovered, just as hackers had done during the cyberattack that occurred the previous year."); *id.* ¶¶ 85-89 (noting that poor authentication measures and inadequate networking caused and aggravated the TALX breach).

custody.[330] Thus, Equifax understood that these deficiencies contributed to prior breaches. These prior breaches demonstrated the same, repeated network failures, and contrary to the Defendants' assertions, did depict fundamental problems in Equifax's cybersecurity.

Nonetheless, the Plaintiff has failed to allege that the Individual Defendants, except for Smith, knew, or were severely reckless to the fact that, these prior breaches were symptomatic of fundamental security problems. Although the Plaintiff adequately alleges that these prior breaches involved some of the same problems involved in the Data Breach, it has not alleged that Gamble, Dodge, or Ploder had specific knowledge, or access to specific facts, informing them that these prior breaches involved these specific issues. Absent such allegations, the Plaintiff has failed to allege that the Individual Defendants other than Smith knew that the prior breaches involved these authentication and monitoring issues, or that they were severely reckless as to this fact. Without knowing that these breaches were specifically caused by authentication and network monitoring issues, these Defendants would not have been put on notice that there were shortcomings in these areas of security. Without this knowledge, these previous breaches do not serve as warnings of the many

---

[330] *Id.* ¶ 70 ("In its March 2014 letter, Equifax assured the New Hampshire Attorney General that the Company would implement 'additional monitoring and blocking measures' to protect at-risk information.").

cybersecurity deficiencies that the Plaintiff alleges in the Amended Complaint, and thus cannot establish scienter.

However, these prior breaches do help establish scienter as to Smith. As explained above, Equifax hired Mandiant in early 2017 in response to the TALX breach.[331] Smith personally oversaw and closely monitored this investigation by Mandiant.[332] Mandiant then confirmed in its review that Equifax's systems were grossly inadequate, and warned that Equifax's failure to patch vulnerabilities could present problems. Thus, Smith was personally aware of Mandiant's investigation and the results of this investigation, and knew that this investigation had been initiated due to the prior TALX breach. Thus, these allegations are sufficient to infer that Smith knew, or was severely recklessly as to the fact that, the TALX breach was the result of deficiencies in Equifax's cybersecurity. Therefore, the Court concludes that the TALX breach along with Mandiant's audit report contribute to a finding of scienter as to Smith. According to the Amended Complaint, the Mandiant investigation was a "top-secret project" that Smith was "overseeing personally."[333] Smith, at least, had access to facts showing that the cybersecurity was seriously deficient, which

---

331 Am. Compl. ¶ 91.

332 *Id.*

333 Am. Compl. ¶ 91.

would contribute to a conclusion that he was at least severely reckless in making statements touting Equifax's cybersecurity.

2. Knowledge of the Data Breach

Next, the Plaintiffs argue that Equifax Senior Management's knowledge of the Data Breach raises a strong inference of scienter.[334] In the Amended Complaint, the Plaintiff alleges that Senior Management, including the Individual Defendants were "well aware" of the Data Breach by "late July 2017," but nonetheless failed to disclose the incident and continued to make false statements concerning Equifax's data security.[335] Thus, according to the Plaintiff, the Defendants knowingly or recklessly made false statements because they knew of the Data Breach. The Defendants argue that these allegations concerning the Defendants' knowledge of the Data Breach fail to give rise to a strong inference of scienter.[336]

First, the Defendants argue that each of the challenged statements attributed to Gamble, Ploder, and Dodge, and all but one of the statements attributed to Smith, are alleged to have been made on or before July 27, 2017.[337] Thus, as to these statements, the Individual Defendants could not have known or been severely reckless as to the risk of misleading investors since they did not

---

334 Pl.'s Br. in Opp'n to Defs.' Mot. to Dismiss, at 47.

335 Am. Compl. ¶ 272.

336 Defs.' Mot. to Dismiss, at 44.

337 *Id.* at 44.

know of the existence of the Data Breach. The Court agrees. The Plaintiff has not shown that Gamble, Dodge, or Ploder made any of the challenged statements after they allegedly became aware of the Data Breach in late July 2017.[338] Thus, these Individual Defendants' knowledge of the Data Breach does not establish scienter as to any of their specific alleged violations.

However, these allegations do support a finding of scienter as to Smith. On August 16, 2017, after discovery of the Data Breach, Smith made comments regarding Equifax's data security in a speech at the University of Georgia.[339] The factual allegations in the Amended Complaint support a finding that Smith made these statements with the requisite scienter. By this point, Mandiant had already informed Smith that it was likely that a large amount of personally identifiable information had been compromised in the Data Breach.[340] Furthermore, Smith had personally overseen the previous Mandiant investigation in March 2017, in which Mandiant concluded that Equifax's cybersecurity practices were grossly inadequate.[341] Thus, Smith, despite knowing that the sensitive data had been compromised in the Data Breach, and despite personally overseeing this previous investigation by Mandiant,

---

[338] At the earliest, according to the Complaint, the Defendants became aware of the Data Breach on July 29, 2017. *See, e.g.*, Am. Compl. ¶ 15.

[339] Am. Compl. ¶ 334.

[340] *Id.* ¶ 122.

[341] *Id.* ¶¶ 91-92.

nonetheless stated that data security is "a huge priority for us" and that it was his "number one worry."[342] These allegations are sufficient to raise a strong inference that Smith made this statement with the requisite scienter.

The Defendants argue that, even assuming Smith was aware of the Data Breach when he made this statement, "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.'"[343] However, these arguments do not address whether Smith acted with the necessary scienter. Instead, they ask whether the statements were false or misleading – which is a separate inquiry. The Defendants conflate the two issues. As discussed above, these statements were false or misleading because a reasonable investor would understand this statement to convey that there was no significant security breach when it was made. The Defendants also argue that scienter as to this statement is not adequately alleged because the Plaintiff did not plead facts that Smith knew the statements were false or misleading. However, as explained above, Smith made these statements despite his knowledge of Mandiant's warnings concerning Equifax's deficiencies. Such knowledge, even if Smith disagreed with it, contributes to an inference of recklessness.

3. Core Business Operation

---

342 *Id.* ¶ 334.

343 Defs.' Mot. to Dismiss, at 45.

The Plaintiffs next argue that the fact that the alleged violations concerned one of the most critical risks facing Equifax contributes to a strong inference of scienter.[344] However, the fact that an alleged fraud concerned a company's core business does not itself establish a strong inference of scienter. "[I]t is not automatically assumed that a corporate officer is familiar with certain facts just because these facts are important to the company's business; there must be other, individualized allegations that further suggest that the officer had knowledge of the fact in question."[345] Instead, "a person's status as a corporate officer, when considered alongside other allegations, can help support an inference that that person is familiar with the company's most important operations."[346]

However, this argument fails to establish scienter.[347] It is insufficient for a plaintiff to make "conclusory allegations that the Defendants had access to the 'true facts' in order to demonstrate scienter, particularly where the complaint fails to allege 'which defendant knew what, how they knew it, or when.'"[348] The

---

[344] Pl.'s Br. in Opp'n to Defs.' Mot. to Dismiss, at 48.

[345] *In re Heartland Payment Sys., Inc. Sec. Litig.*, Civ. No. 09-1043, 2009 WL 4798148, at *7 (D.N.J. Dec. 7, 2009).

[346] *Id.*

[347] *See In re Coca-Cola Enters. Sec. Litig.*, 510 F. Supp. 2d 1187, 1200-01 (N.D. Ga. 2007) ("[T]he Plaintiffs have failed to plead facts sufficient to demonstrate that the Defendants engaged in channel stuffing.").

[348] *Id.* at 1201 (quoting *In re Theragenics Corp. Sec. Litig.*, 105 F. Supp. 2d 1342, 1361 (N.D. Ga. 2000)).

Plaintiff's allegations that cybersecurity was critical to Equifax's business operations fail to establish scienter as to Dodge, Ploder, and Gamble. The Plaintiff must plead specific facts establishing that the Individual Defendants knew of, or were severely reckless as to, the existing deficiencies in Equifax's data systems. General allegations that cybersecurity is critical to Equifax's business may, in totality, contribute to a finding of scienter. However, absent allegations that Gamble, Ploder, or Dodge had access to specific facts showing these problems, this argument fails.

The Eleventh Circuit's decision in *Garfield v. NDC Health Corporation* is instructive.[349] There, the plaintiff alleged that the defendants attended monthly operations meetings where every aspect of the business was discussed in detail, including "the aggressive channel stuffing and mounting problems with accounts recevable (sic)" that were at the center of the plaintiff's fraud allegations.[350] The plaintiff also alleged that testimonial evidence by a former senior executive would show that the defendants knew of these problems.[351] The court concluded that these allegations failed to establish scienter due to the absence of "particularized averments of fraud or scienter."[352] The plaintiff's broad claims lacked the requisite detail because "it failed to allege what was

---

349 *Garfield v. NDC Health Corp.*, 466 F.3d 1255 (11th Cir. 2006).

350 *Id.* at 1264.

351 *Id.*

352 *Id.* at 1265.

said at the meeting, to whom it was said, or in what context."[353] The court explained that "[a] general allegation that Individual Defendants promoted channel stuffing at a series of meetings does not establish scienter."[354]

Here, the Plaintiff fails to establish a strong inference of scienter based upon Dodge, Ploder, and Gamble's roles in the company. The Amended Complaint fails to allege what warnings were given to each of these specific Individual Defendants, when those warnings were conveyed to these Individual Defendants, what was said in such warnings, and in what context those warnings were made.[355] Generally, the Plaintiff alleges that these Individual Defendants, based upon their positions and their general duty to monitor the operations of Equifax's networks and systems, must have known about the deficient state of its cybersecurity. The Amended Complaint, however, fails to provide specific factual allegations as to a "time, place or manner" in which any of the Individual Defendants were specifically warned of these cybersecurity deficiencies.[356] Therefore, these allegations are insufficient to support an inference of scienter.

---

[353] *Id.*

[354] *Id.*

[355] *In re Coca-Cola Enters. Sec. Litig.*, 510 F. Supp. 2d 1187, 1201 (N.D. Ga. 2007).

[356] *Id.* ("The Amended Complaint fails to provide any specific allegations regarding a time, place or manner in which any of the Individual Defendants was specifically informed or indicated special knowledge as to CCE's channel stuffing activities.").

The Plaintiff cites *In re Ebix, Inc. Securities Litigation.* There, the court concluded that the factual allegations gave rise to a strong inference that the defendants were at least severely reckless in their representations due to the defendants' "roles within the company (CEO and CFO), their active participation in press releases, earnings calls, and SEC filings dealing with the issues focused on in the [complaint], and the nature, duration and extent of the fraud alleged."[357] However, *Ebix* is distinguishable from this case because there the plaintiff alleged "specific communications to and from the Individual Defendants regarding these issues."[358] In contrast, the Plaintiff here has not alleged any specific communications to or from any of the Individual Defendants concerning the state of Equifax's cybersecurity. Without these types of specific allegations, the Plaintiff fails to establish a strong inference that the Individual Defendants were severely reckless in their representations concerning Equifax's data security.

Thus, these general allegations that cybersecurity was a core business operation do not support an inference that Dodge, Gamble, or Ploder knowingly or recklessly misrepresented the state of Equifax's networks when they stated that cybersecurity was one of Equifax's top priorities. These allegations do contribute to a finding of scienter as to Smith, when taken into account with the

---

357 *Ebix*, 898 F. Supp. 2d at 1346-47.

358 *Id.* at 1347.

other, more specific allegations as to his knowledge of problems with Equifax's data security. However, on their own, these allegations do not establish a strong inference of scienter.

4. Defendants' Assurances

Next, the Plaintiff argues that the Defendants assured investors that they were focused on cybersecurity and compliance with data security laws, and that these assurances support an inference of scienter.[359] The Plaintiff cites *In re Theragenics Corp. Securities Litigation* in support of this argument.[360] However, the facts of that case are distinguishable. This Court in *Theragenics* did not hold that the defendants' assurances that they were monitoring their competitor's performance supported an inference of scienter. Instead, the plaintiffs there alleged that the defendants did in fact continually monitor the performance of their competitor, establishing that they knew their statements were false or misleading. In contrast, the Plaintiff here has not shown that the Individual Defendants, aside from Smith, were monitoring Equifax's cybersecurity or had access to specific information or warnings that would have established that they knew or were severely reckless as to the falsity of the statements they made.

In essence, the Plaintiff argues that the Defendants stated that they were closely monitoring Equifax's cybersecurity, and that from this, one can infer that

---

[359] Pl.'s Br. in Opp'n to Defs.' Mot. to Dismiss, at 50.

[360] *In re Theragenics Corp. Sec. Litig.*, 137 F. Supp. 2d 1339, 1348 (N.D. Ga. 2001).

they must have known about the problems with data security. However, the fact that the Defendants stated that they were closely monitoring Equifax's network security does not establish that they knew of, or were severely reckless to the existence of, these cybersecurity deficiencies. These allegations are too general. Instead, the more plausible inference is that the Individual Defendants, besides Smith, were negligent with regard to their management and monitoring of cybersecurity. In the cases relied upon by the Plaintiff, the plaintiffs alleged that the defendants *were* in fact monitoring the events underlying the false or misleading statements, and thus knew or were severely reckless to the fact that the statements made were false.[361] Scienter was not established in those cases merely because the defendants assured investors that they were monitoring those underlying events, as the Plaintiff here alleges. This argument, which requires additional inferential steps, is insufficient to establish scienter as to Gamble, Ploder, and Dodge.

5. Egregiousness of Cybersecurity Deficiencies

---

[361] *See In re Immucor Inc. Sec. Litig.*, No. 1:05-CV-2276-WSD, 2006 WL 3000133, at *18 (N.D. Ga. Oct. 4, 2006) ("That Gallup never disclosed the full scope of the Italian situation, even after it is apparent that he knew of its scope and gravity, lends strength to the inference that Gallup intentionally or recklessly withheld from investors a full and fair statement of the problems in Italy and their possible consequences."); *In re Theragenics Corp. Sec. Litig.*, 137 F. Supp. 2d 1339, 1348 (N.D. Ga. 2001) (noting that the plaintiffs' scienter claim was based, in part, on their "claim that Theragenics closely and continually monitored the performance of Amersham, its largest competitor").

The Defendants next contend that the Plaintiff's allegations as to the "egregiousness" of the shortcomings in Equifax's data security fail to support a strong inference of scienter.[362] Instead, according to the Defendants, these allegations merely constitute hindsight criticism as to the manner in which Equifax managed cybersecurity.[363] The Plaintiff argues that the magnitude, scope, and duration of the deficiencies in Equifax's cybersecurity systems were such that they could not have escaped the notice of the Defendants and other senior management, and that this supports an inference of scienter.[364] And, according to the Plaintiff, this is compounded by the fact that the Defendants allegedly represented that they were "closely monitoring" Equifax's data security.[365] The Court concludes, however, that the egregiousness of Equifax's cybersecurity problems, without more specific allegations, fails to establish scienter. Once again, as discussed above, the Plaintiff has failed to establish that Dodge, Gamble, or Ploder knew of or were severely reckless as to these egregious deficiencies. The severity of these problems, if taken into account with other specific factual allegations supporting scienter, could help establish an inference of scienter. However, here those other allegations are absent. Without those allegations, the Plaintiff has failed to establish an inference that is cogent

---

362 Defs.' Mot. to Dismiss, at 46-47.

363 *Id.*

364 Pl.'s Br. in Opp'n to Defs.' Mot. to Dismiss, at 51.

365 *Id.* at 51.

and compelling, and just as likely as other, more innocent explanations. Even if these problems were severe and widespread, it is still more plausible to infer that these Individual Defendants were negligent, rather than something more insidious.

6. Stock Sales

Next, the Plaintiff argues that suspicious stock sales by Gamble and Ploder support an inference of scienter. "[T]he timing of stock trades by insiders also may be relevant to inferring scienter."[366] "Stock sales or purchases timed to maximize returns on nonpublic information weigh in favor of inferring scienter; the lack of similar sales weighs against inferring scienter."[367] "To demonstrate the relevance of stock trades to the issue of scienter, a plaintiff 'bear[s] the burden of showing that sales by insiders were in fact unusual or suspicious in amount and in timing.'"[368]

Here, the Court concludes that the stock sales fail to establish scienter. First, the Plaintiff fails to allege that any of the other Individual Defendants, including Smith, the CEO, engaged in insider trading. This alone undermines any inference that these stock sales contribute to a finding of scienter.[369] Second,

---

366 *Mizarro v. Home Depot, Inc.*, 544 F.3d 1230, 1253 (11th Cir. 2008).

367 *Id.*

368 *In re Coca-Cola Enters. Inc. Sec. Litig.*, 510 F. Supp. 2d 1187, 1202 (N.D. Ga. 2007) (quoting *Druskin v. Answerthink, Inc.*, 299 F. Supp. 2d 1307, 1335 (S.D. Fla. 2004)).

369 *Id.*

the stock sales, which can constitute circumstantial evidence that Gamble and Ploder knew that Equifax's stock price was artificially inflated, cannot *on their own* establish scienter as to these Defendants. However, as discussed above, the Plaintiff has failed to provide more than general allegations that any of the Individual Defendants, besides Smith, made misstatements with knowledge or severe recklessness toward their falsity. This circumstantial evidence fails to meet the stringent pleading requirements under the PSLRA that the allegations give rise to a strong inference of scienter.

There is no doubt that these sales by Gamble and Ploder are suspicious, especially given their timing. They contribute to an inference of scienter, but they are not sufficient *on their own* to raise a strong inference of scienter with regard to Gamble and Ploder as to the alleged violations.[370] The stock sales could have, when aggregated with other facts, contributed to a finding of a strong inference of scienter. However, they cannot establish this strong inference on their own.[371] This is compounded by the fact that the other Individual Defendants, including Smith, did not engage in similarly suspicious stock

---

[370] *In re Spectrum Brands, Inc. Sec. Litig.*, 461 F. Supp. 2d 1297, 1318 (N.D. Ga. 2006) ("The sales contribute to an inference of scienter as to Jones, but are not alone sufficient to raise a strong inference that Jones acted with scienter in committing the acts of securities fraud alleged.").

[371] *In re Theragenics Corp. Sec. Litig.*, 105 F. Supp. 2d 1342, 1361 (N.D. Ga. 2000) ("[T]he Plaintiffs in this case cannot base scienter on stock sales alone. The stock sales *may* constitute circumstantial evidence that Defendants Jacobs and Smith knew Theragenics' stock price was artificially inflated and may support a strong inference of scienter.").

sales.[372] Thus, given the lack of other specific factual allegations establishing scienter as to these Defendants, the suspicious stock sales by Gamble and Ploder fail to give rise to a strong inference of scienter on their own.

7. Sudden Resignations of Equifax Officers

Next, the Plaintiff contends that the sudden departures of high-ranking Equifax executives support an inference of scienter.[373] On September 15, 2017, about a week after public disclosure of the Data Breach, Chief Security Officer Susan Mauldin and Chief Information Officer David Webb resigned from Equifax.[374] On September 26, 2017, Smith retired from Equifax, without severance, effective immediately.[375] The Equifax Board of Directors announced that it had the power to retroactively classify Smith as having been fired for cause, which includes intentional or reckless misconduct.[376] According to the Plaintiff, the circumstances surrounding these departures of senior executives establish a strong inference that "there were profound failures in [Equifax's] data protection practices that were the result of reckless or intentional misconduct."[377]

---

372 *Coca-Cola*, 510 F. Supp. 2d at 1202.

373 Pl.'s Br. in Opp'n to Defs.' Mot. to Dismiss, at 53-54.

374 Am. Compl. ¶ 280.

375 *Id.* ¶ 281.

376 *Id.*

377 *Id.* ¶ 282.

Some courts have concluded that the resignation of corporate officers, in certain contexts, can support an inference of scienter.[378] However, in those cases, the context of the executives' resignations was important. The fact that an executive resigned, on its own, does not support an inference of scienter. Instead, the circumstances of the resignation must suggest that intentional or reckless misconduct had occurred. For example, in *In re Home Loan Servicing Solutions, Ltd. Securities Litigation*, cited by the Plaintiff, the court concluded that scienter was established as to a defendant who, among other things, was "at the epicenter" of the business, who was "forced to resign," and who regulatory documents indicated was "engaged in improper transactions."[379] Similarly, in *In re OSG Securities Litigation*, the court concluded that the resignations of two executives supported an inference of scienter when the "circumstances and timing of the resignations" suggest that both defendants were terminated in relation to the undisclosed tax issue underlying the fraud claims.[380] The court noted that "[a]lthough the decision to terminate the

---

[378] *See, e.g.*, *In re Home Loan Servicing Sols., Ltd. Sec. Litig.*, No. 16-cv-60165-WPD, 2016 WL 10592320, at *7 (S.D. Fla. June 6, 2016) (noting that the fact that a corporate officer "was forced to resign" contributed to a finding of scienter); *In re OSG Sec. Litig.*, 12 F. Supp. 3d 622, 632 (S.D.N.Y. 2014) (" The circumstances and timing of the resignations suggest that both defendants were 'terminated in relation to the undisclosed tax issue.'").

[379] *In re Home Loan Servicing Sols., Ltd. Sec. Litig.,* 2016 WL 10592320, at *7.

[380] *In re OSG Sec. Litig.*, 12 F. Supp. 3d at 632.

defendants does not negate the possibility of mere negligence in mismanaging the Section 956 issue, it more likely suggests a higher level of wrongdoing approaching recklessness or even conscious malfeasance."[381]

In contrast, the context of the resignations here does not suggest that Gamble, Ploder, or Dodge knew of, or were severely reckless as to, the false or misleading nature of their statements. The Plaintiff fails to explain how the resignations of Smith, Mauldin, and Webb show that Gamble, Ploder, or Dodge acted with the requisite state of mind. Nothing about the context of these resignations would lead one to infer that Gamble, Ploder, or Dodge must have known about the deficient state of Equifax's cybersecurity. Without such allegations, the resignations of Smith, Mauldin, and Webb fail to establish scienter as to these Individual Defendants.

However, Smith's resignation does contribute to a finding of scienter on his part. Taking all of these allegations into account, the following facts support a strong inference of scienter: Smith was warned by Mandiant, after a previous breach, that Equifax's cybersecurity was grossly inadequate; Smith, as CEO, would have likely followed many of the developments in Equifax's cybersecurity since it was an important aspect of its business; Smith learned of the Data Breach in late July 2017, but still continued to make statements touting the company's security; and after the public disclosure of the incident, Smith

---

[381] *Id.* at 632-33.

resigned his roles in the company, while the Board of Directors announced it may decide to retroactively terminate him "with cause." These allegations, taken together, give rise to a strong inference of scienter that Smith made these misstatements with knowledge or severe recklessness as to their falsity.

But, the Court concludes overall that the Plaintiff has failed to allege specific facts giving rise to a strong inference of scienter as to Gamble, Ploder, or Dodge. Instead, as to these Defendants, the Plaintiff relies upon inferences based upon their role in the company and the size of the fraud. These general allegations do not suffice. "[I]t is not enough to make conclusory allegations that the Defendants had access to the 'true facts' in order to demonstrate scienter, particularly where the complaint fails to allege 'which defendant knew what, how they knew it, or when.'"[382] "Nor does a vague assertion that a defendant must have known about the fraud by virtue of his position of authority suffice to prove a strong inference of scienter."[383] Without specific allegations that Gamble, Ploder, and Dodge had access to information that made them aware of the problems with Equifax's data security, the Amended Complaint fails to give rise to a strong inference of scienter as to these Individual Defendants. Thus,

---

[382] *In re Coca-Cola Enters. Inc. Sec. Litig.*, 510 F. Supp. 2d 1187, 1201 (N.D. Ga. 2007) (quoting *In re Theragenics Corp. Sec. Litig.*, 105 F. Supp. 2d 1342, 1361 (N.D. Ga. 2000)).

[383] *Orton v. Parametric Tech. Corp.*, 344 F. Supp. 2d 290, 306 (D. Mass. 2004).

the Plaintiff fails to adequately plead scienter under the stringent requirements set forth in the PSLRA.[384]

8. Equifax's State of Mind

Finally, the Defendants argue that the Plaintiff has failed to adequately plead scienter as to Equifax.[385] However, failure to adequately plead scienter as to individual defendants does not automatically mean that scienter cannot be established against a corporation.[386] "Corporations, of course, have no state of mind of their own. Instead, the scienter of their agents must be imputed to them."[387] A plaintiff, in theory, can still create a strong inference that a corporate defendant such as Equifax acted with the requisite scienter, even if

---

[384] *See In re Coca-Cola Enters. Inc. Sec. Litig.*, 510 F. Supp. 2d 1187, 1201 (N.D. Ga. 2007) ("Here, the Plaintiffs similarly fail to allege that any of the Defendants had knowledge as to the channel stuffing. The essence of their allegations is that because of the Defendants' positions and their general duty to monitor the information on Margin Minder, the Defendants must have known about the channel stuffing. The Amended Complaint fails to provide any specific allegations regarding a time, place or manner in which any of the Individual Defendants was specifically informed or indicated special knowledge as to CCE's channel stuffing activities. These pleadings are thus insufficient to demonstrate an inference of scienter.").

[385] Defs.' Mot. to Dismiss, at 53-54.

[386] *Mizzaro*, 544 F.3d at 1254 ("Even though it failed to plead scienter adequately for any of the individual defendants, the amended complaint could, in theory, still create a strong inference that the corporate defendant, Home Depot, Inc., acted with the requisite state of mind."); *see also Plymouth Cty. Ret. Sys. v. Carter's Inc.*, No. 1:08-cv-02940-JOF, 2011 WL 13124501, at *12 n.8 (N.D. Ga. Mar. 17, 2011).

[387] *Mizzaro*, 544 F.3d at 1254.

it has failed to prove scienter as to the individual defendants.[388] Even if the Amended Complaint fails to raise a strong inference of scienter as to any of the named Individual Defendants, the Plaintiff can survive dismissal if it "raise[s] a strong inference that *somebody* responsible for the allegedly misleading statements must have known about the fraud."[389] To do so, the Plaintiff must allege facts in the Amended Complaint creating a strong inference that unnamed Equifax officials "were both responsible for issuing the allegedly false public statements and were aware of the alleged fraud."[390] It can do so through allegations relating the state of mind of corporate officials "who make or issue the statement (or order or approve it or its making or issuance, or who furnish information or language for inclusion therein, or the like)."[391]

Here, the Plaintiff's claims as to Equifax survive to the extent that the claims against Smith survive dismissal. Furthermore, the Plaintiff has alleged that Equifax's employees warned "management" of the deficient state of the company's cybersecurity. While these allegations are insufficient to establish scienter as to the named Defendants other than Smith, they are sufficient to establish that *some* corporate officials at Equifax, who would have had a role in

---

388 *Mizzaro*, 544 F.3d at 1254.

389 *Mizzaro*, 544 F.3d at 1254 (emphasis in original).

390 *Id.* at 1254-55.

391 *Id.* at 1254 (quoting *Southland Sec. Corp. v. INSpire Ins. Sols., Inc.*, 365 F.3d 353, 366 (5th Cir. 2004)).

crafting many of the statements made by the company, knew of the data security problems in the company. This is especially true given the resignations of Webb and Mauldin, two corporate executives whose responsibilities included data security, and Smith, whose role as CEO would have encompassed data security. The Plainitff alleges that Equifax employees warned "management" of the problems with the company's cybersecurity, and also alleges that Webb and Mauldin resigned after the Data Breach. This supports an inference that *some* corporate officials in Equifax knew, or were severely reckless, as to the fraudulent conduct. Thus, the Court concludes that the Amended Complaint still creates a strong inference that Equifax, the corporate defendant, acted with the requisite state of mind.[392]

C. Loss Causation

Next, the Defendants argue that the Plaintiff has failed to adequately allege loss causation.[393] The Plaintiff must allege facts demonstrating that the Defendants' misrepresentations caused the losses for which the Plaintiff seeks to recover.[394] To prove loss causation in a section 10(b) claim, "a plaintiff must offer 'proof of a causal connection between the misrepresentation and the

---

392 *Id.*

393 Defs.' Mot. to Dismiss, at 54.

394 *See* 15 U.S.C. § 78u-4(b)(4).

investment's subsequent decline in value.'"[395] Essentially, the Plaintiff must show that the Defendants' fraud, and not some other factor, proximately caused its alleged losses.[396] The loss causation element does not require a plaintiff to prove that a "fraudulent misrepresentation was the *sole* cause of a security's loss in value."[397] But, "the plaintiff must still demonstrate that the fraudulent statement was a 'substantial' or 'significant' cause of the decline in price."[398] "By ensuring that only losses actually attributable to a given misrepresentation are cognizable, the loss causation requirement ensures that the federal securities laws do not 'becom[e] a system of investor insurance that reimburses investors for any decline in the value of their investments.'"[399] Section 10(b) is not a "prophylaxis" against the normal risks associated with investment in the stock market, but instead is designed solely to protect against fraud.[400] The loss causation element is only subject to Rule 8's notice pleading standard, requiring

---

[395] *Meyer v. Greene*, 710 F.3d 1189, 1195 (11th Cir. 2013) (quoting *Robbins v. Koger Props., Inc.*, 116 F.3d 1441, 1448 (11th Cir. 1997)).

[396] *FindWhat Inv'r Grp. v. FindWhat.com*, 658 F.3d 1282, 1309 (11th Cir. 2011).

[397] *Meyer*, 710 F.3d at 1196 (citing *Hubbard v. BankAtlantic Bancorp, Inc.*, 688 F.3d 713, 726 (11th Cir. 2012)).

[398] *Id.* (citing *Hubbard*, 688 F.3d at 726).

[399] *Meyer*, 710 F.3d at 1196 (quoting *Robbins v. Koger Props., Inc.*, 116 F.3d 1441, 1447 (11th Cir. 1997)).

[400] *Id.*

a "short and plain" statement, and not the heightened pleading standards of the PSLRA.[401]

In the Amended Complaint, the Plaintiff alleges that "the market for Equifax's securities was efficient" and that "the market for Equifax stock promptly digest current information regarding Equifax from all publicly available sources and reflected such information in Equifax's stock price."[402] Thus, according to the Plaintiff, it is entitled to a presumption of reliance. The Plaintiff's claims therefore rely upon the fraud-on-the-market theory of causation, derived from the efficient market hypothesis.[403] This hypothesis provides "that 'in an open and developed securities market, the price of a company's stock is determined by the available material information regarding the company and its business.'"[404] "Because millions of shares change hands daily, and a critical mass of market makers study the available information and influence the stock price through trades and recommendations, an efficient capital market rapidly and efficiently digests all available information and translates that information into the processed form of a market price."[405] "Just

---

401 *Id.*

402 Am. Compl. ¶¶ 363-64.

403 *FindWhat Inv. Grp.*, 658 F.3d at 1309-10.

404 *Id.* at 1310 (quoting *Basic Inc. v. Levinson*, 485 U.S. 224, 241 (1988)).

405 *Id.* (internal quotations and citations omitted).

as an efficient market translates all available truthful information into the stock price, the market processes the publicly disseminated falsehood and prices it into the stock as well."[406] "The market price of the stock will then include an artificial 'inflationary' value—the amount that the market mistakenly attributes to the stock based on the fraudulent misinformation."[407]

This presumption is also relevant for loss causation. "While reliance focuses on the front-end causation question of whether the defendant's fraud induced or influenced the plaintiff's stock purchase, loss causation provides the 'bridge between reliance and actual damages.'"[408] In a fraud-on-the-market case, the loss causation element requires the plaintiff to show "that the fraud-induced inflation that was baked into the plaintiff's purchase price was subsequently removed from the stock's price, thereby causing losses to the plaintiff."[409] Plaintiffs often demonstrate loss causation in fraud-on-the-market cases circumstantially, by:

---

406 *Id.*

407 *Id.*

408 *FindWhat Inv. Grp.*, 658 F.3d at 1311 (quoting *In re Cooper Cos. Sec. Litig.*, 254 F.R.D. 628, 638 (C.D. Cal. 2009)); *see also In re Williams Sec. Litig.*, 558 F.3d 1130, 1137 (10th Cir. 2009) ("Loss causation is easiest to show when a corrective disclosure reveals the fraud to the public and the price subsequently drops—assuming, of course, that the plaintiff could isolate the effects from any other intervening causes that could have contributed to the decline.").

409 *Id.*

> (1) identifying a "corrective disclosure" (a release of information that reveals to the market the pertinent truth that was previously concealed or obscured by the company's fraud); (2) showing that the stock price dropped soon after the corrective disclosure; and (3) eliminating other possible explanations for this price drop, so that the factfinder can infer that it is more probable than not that it was the corrective disclosure—as opposed to other possible depressive factors—that caused at least a "substantial" amount of the price drop.[410]

Overall, "loss causation analysis in a fraud-on-the-market case focuses on the following question: even if the plaintiffs paid an inflated price for the stock as a result of the fraud (i.e., even if the plaintiffs relied), did the relevant truth eventually come out and thereby cause the plaintiffs to suffer losses?"[411]

The Defendants argue that the announcements to the public of the Data Breach on and following September 7, 2017 did not "reveal" that the prior statements concerning Equifax's data security were false, and thus were not a corrective disclosure.[412] Specifically, the Defendant contends that: (1) the initial announcement of the incident on September 7, 2017 did not reveal that prior statements referencing Equifax's commitment to data security, efforts to protect data, and compliance with laws and regulations were false; (2) the revelations on September 11, 2017 that Equifax lacked an effective data breach crisis management plan did not show that any of the challenged statements were false

---

410 *Id.* at 1311-12 (footnote omitted).

411 *Id.* (citing *Dura Pharm., Inc. v. Broudo*, 544 U.S. 336, 347 (2005)).

412 Defs.' Mot. to Dismiss, at 55.

or misleading; (3) the revelations on September 12, 2017 that 11.5 million customers signed up for the identity protection plan offered by Equifax does not reveal the falsity of any prior statements; and (4) revelations on September 13 and 14, 2017 that the Apache Struts vulnerability caused the Data Breach did not reveal that any of the challenged statements were false or misleading.[413]

However, as noted above, a disclosure need not precisely mirror an earlier misrepresentation, but instead must relate to the misrepresentation and not other negative information about the company.[414] Furthermore, a corrective disclosure can come from any source, and can take any form from which the market would absorb the information and accordingly react.[415] The Court concludes that the Plaintiff has adequately alleged loss causation. "Rule 8 is satisfied if plaintiff provides 'a short and plain statement adequate to give defendants some indication of the loss and the causal connection that the plaintiff has in mind.'"[416] The Plaintiff alleges that the initial disclosure of the Data Breach, along with subsequent disclosures that Equifax's poor cybersecurity played a part in the incident, that Congress would be conducting

---

413 *Id.* at 56-57.

414 *Meyer*, 710 F.3d at 1197.

415 *FindWhat Investor Grp. v. FindWhat.com*, 658 F.3d 1282, 1312 n.28 (11th Cir. 2011).

416 *In re Ebix, Inc. Sec. Litig.*, 898 F. Supp. 2d 1325, 1347 (N.D. Ga. 2012) (quoting *In re Coca-Cola Enters. Inc. Sec. Litig.*, 510 F. Supp. 2d 1187, 1203-04 (N.D. Ga. 2007)).

a probe into Equifax's general cybersecurity practices, that millions of consumers were affected, and that a failure to implement a patch that had been available since March 2017 caused the Data breach, all combined to disclose the truth to investors. This, along with the wide variety of news reporting on the incident detailing Equifax's cybersecurity problems, slowly revealed the truth about the prior misstatements. This adequately puts the Defendants on notice as to the causal connection between the Defendants' misrepresentations and the class's losses.

The Plaintiff also argues that a corrective disclosure "may occur through the materialization of an event within the 'zone of risk' concealed by defendant's misstatements."[417] Under this theory, "[i]f the significance of the truth is such as to cause a reasonable investor to consider seriously a zone of risk that would be perceived as remote or highly unlikely by one believing the fraud, and the loss ultimately suffered is within that zone, then a misrepresentation or omission as to that information may be deemed a foreseeable or proximate cause of the loss."[418] The Eleventh Circuit "has never decided whether the materialization-of-concealed-risk theory may be used to prove loss causation in

---

417 Pl.'s Br. in Opp'n to Defs.' Mot. to Dismiss, at 58.

418 *Lentell v. Merrill Lynch & Co.*, 396 F.3d 161, 173 (2d Cir. 2005) (quoting *Castellano v. Young & Rubicam, Inc.*, 257 F.3d 171, 188 (2d Cir. 2001)).

a fraud-on-the-market case."[419] The Court declines to adopt this theory here. First, the Plaintiff failed to plead this theory of loss causation in the Amended Complaint. Second, the Plaintiff has failed to explain *how* the "materialization" of the Data Breach itself corrected prior misstatements touting the strength of Equifax's cybersecurity. Third, the Court need not adopt this theory since the Plaintiff has adequately alleged loss causation through corrective disclosures.

D. In Connection With

Next, the Defendants contend that the statements made by Smith in a speech at the University of Georgia were not made in connection with the purchase or sale of a security.[420] To state a claim under section 10(b), the

---

[419] *Sapssov v. Health Mgmt. Assocs., Inc.*, 608 F. App'x 855, 861 n.7 (11th Cir. 2015) (quoting *Hubbard v. BankAtlantic Bancorp, Inc.*, 688 F.3d 713, 726 n.25 (11th Cir. 2012)).

[420] Defs.' Mot. to Dismiss, at 45 n.18. At oral argument, counsel for the Defendants devoted a significant portion of his time arguing that the challenged statements published on Equifax's website were not made "in connection" with the sale or purchase of a security. *See* Transcript of Oral Argument, at 20-23 [Doc. 83]. However, this argument was not raised in the Defendants' papers. Instead, the Defendants only assert in their papers that Smith's statements at the University of Georgia were not made in connection with the purchase or sale of a security. *See* Defs.' Mot. to Dismiss, at 45 n.18; Defs.' Reply Br., at 21 n.12. The Defendants' failure to raise this argument in their briefs means that the argument has been abandoned. *See Access Now, Inc. v. Sw. Airlines Co.*, 385 F.3d 1324, 1330 (11th Cir. 2004) ("[A] legal claim or argument that has not been briefed before the court is deemed abandoned and its merits will not be addressed."). And, even if the Defendants had raised this argument, the Court would not be persuaded. As discussed below, even statements made in technical jargon in a sophisticated medical journal can be considered "in connection with" the purchase or sale of a security, since analysts search for such information in evaluating stocks. *See In re Carter-Wallace, Inc. Sec. Litig.*, 150 F.3d 153, 156 (2d Cir. 1998). Here, the Court cannot say that, as a matter of law, statements

plaintiff must show that the false or misleading statement was made in connection with the purchase or sale of a security.[421] In using this phrase, "Congress . . . 'intended only that the device employed, whatever it might be, be of a sort that would cause reasonable investors to rely thereon, and, in connection therewith, so relying, cause them to purchase or sell a corporation's securities.'"[422] "Moreover, when . . . a claim is based on the fraud-on-the-market theory, a 'straightforward cause and effect' test is applied, under which it is sufficient that 'statements which manipulate the market are connected to resultant stock trading.'"[423]

Here, the Plaintiff has adequately shown that Smith's statement was made in connection with the purchase or sale of a security. "As the Supreme Court has noted, 'market professionals generally consider most publicly announced material statements about companies, thereby affecting stock

---

made on a company's website are not made in connection with a securities transaction, even if those statements are not found prominently on the front page of the company's website. Market analysts, who find such information relevant, are able to locate and digest such information in evaluating a company's stock. *See id.* Therefore, the Court declines to dismiss these website statements for this reason.

[421] *In re Carter-Wallace, Inc. Sec. Litig.*, 150 F.3d 153, 155-56 (2d Cir. 1998).

[422] *Id.* (quoting *SEC v. Tex. Gulf Sulphur Co.*, 401 F.2d 833, 860 (2d Cir. 1968)).

[423] *Id.* (quoting *In re Ames Dep't Stores Inc. Stock Litig.*, 991 F.2d 953, 966 (2d Cir. 1993)).

market prices.'"[424] In *In re Carter-Wallace, Inc. Securities Litigation*, the court noted that "[t]echnical advertisements in sophisticated medical journals detailing the attributes of a new drug could be highly relevant to analysts evaluating the stock of the company marketing the drug," and thus it could not conclude that such statements, as a matter of law, were not made in connection with a securities transaction.[425] Similarly, statements made by Equifax's CEO concerning a core business operation could be highly relevant to analysts evaluating Equifax's stock. The fact that Smith made this statement at a presentation at a college, and not in some other setting, does not change this conclusion. This is further bolstered by the Plaintiff's allegation that this presentation was uploaded to the popular website YouTube.com.[426] The Court cannot say that this statement, which would be relevant to analysts studying Equifax's securities, was not made in connection with a securities transaction. This is especially true given the fact that the Plaintiff relies upon the fraud-on-the-market theory. Therefore, the Court finds the Defendants' argument unpersuasive.

E. Section 20(a) Claims

---

424 *Id.* (quoting *Basic Inc. v. Levinson*, 485 U.S. 224, 247 n.24 (1988)).

425 *Id.*

426 Am. Compl. ¶ 334.

Finally, the Defendants argue that the Plaintiff's section 20(a) claims fail to state a claim for which relief can be granted.[427] Section 20(a) of the Exchange Act extends liability for violations of Rule 10b–5 to controlling persons in the company.[428] "To show control person liability under Section 20(a), a plaintiff must allege that: (1) the company violated § 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."[429]

The Defendants first argue that the Plaintiff's failure to plead any primary violation of section 10(b) by Equifax requires dismissal of the section 20(a) claims.[430] However, as discussed above, the Plaintiff has adequately pleaded some of its section 10(b) claims as to Equifax. The Defendants next argue that the Plaintiff fails to adequately plead that the Individual Defendants control "specific corporate policy" that resulted in the alleged primary violations of section 10(b).[431] Specifically, the Defendants argue that the Plaintiff has not alleged that any of the Individual Defendants had control over the content and

---

427 Defs.' Mot. to Dismiss, at 59.

428 15 U.S.C. § 78t(a).

429 *In re Spectrum Brands, Inc. Sec. Litig.*, 461 F. Supp. 2d 1297, 1307 (N.D. Ga. 2006) (citing *Theoharous v. Fong*, 256 F.3d 1219, 1227 (11th Cir. 2001)).

430 Defs.' Mot. to Dismiss, at 59.

431 *Id.*

dissemination of the unattributed statements made on Equifax's website during the class period, or any of the statements made by different Individual Defendants, or that they controlled the cybersecurity matters misrepresented.[432] Furthermore, the Defendants argue that the Plaintiff has not alleged that Gamble, Ploder, or Dodge controlled Equifax's "general affairs."[433]

The Court agrees that the Plaintiff has failed to allege that Gamble, Ploder, or Dodge exercised control over the specific cybersecurity policies that resulted in the alleged violations, or that they exercised control over any of the unattributed statements made or statements made by other Individual Defendants. Thus, the Plaintiff's section 20(a) claims should be dismissed as to these Individual Defendants. The Court concludes, however, that the Plaintiff has adequately alleged a section 20(a) claim as to Smith. Smith, as CEO, had the power to control the "general affairs" of Equifax. Smith also had the power to control the specific corporate policy that resulted in the section 10(b) violations. Smith had both the power to control Equifax's cybersecurity policy and the statements made by Equifax and the other Individual Defendants as to these cybersecurity policies. Thus, the Plaintiff has sufficiently stated a claim for control liability as to Smith.

---

[432] *Id.* at 59-60.

[433] *Id.* at 60.

IV. Conclusion

For the reasons stated above, the Defendants' Joint Motion to Dismiss [Doc. 62] is GRANTED in part and DENIED in part. It is GRANTED as to the Defendants Gamble, Ploder, and Dodge. It is DENIED as to the Defendants Equifax and Smith.

SO ORDERED, this 28 day of January, 2019.

/s/Thomas W. Thrash
THOMAS W. THRASH, JR.
United States District Judge