IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

IN RE CROWDSTRIKE HOLDINGS, INC. SECURITIES LITIGATION	§ § § § § § § § § § §	1:24-CV-857-RP

ORDER

Before the Court is Defendants' Motion to Dismiss Plaintiff's Consolidated Class Action Complaint. (Dkt. 47). Lead Plaintiff Thomas P. DiNapoli, Comptroller of the State of New York, as Administrative Head of the New York State and Local Retirement System, and as Trustee of the New York State Common Retirement Fund ("Lead Plaintiff") filed a response, (Dkt. 48), and Defendants filed a reply, (Dkt. 55). Plaintiff also filed an Opposition to Defendants' Request for Judicial Notice or Incorporation-By-Reference, (Dkt. 49), and Defendants filed a reply, (Dkt. 56). Having considered the parties' briefs, the record, and the relevant law, the Court enters the following order.

I. BACKGROUND

This case concerns Defendant CrowdStrike Holdings, Inc. ("CrowdStrike"), which is a publicly traded cybersecurity company that sells software "purport[ing] to make its customers safe and secure through reliable and continuous updates." (Compl., Dkt. 41, at 4, 12, 88, 90).[1] Defendant George Kurtz ("Kurtz") is CrowdStrike's Chief Executive Officer ("CEO"), and Defendant Michael

[1] Any references to the Complaint refer to the Consolidated Class Action Complaint for Violations of the Federal Securities Laws, (Dkt. 41).

Sentonas ("Sentonas") is CrowdStrike's President. (*Id.* at 4). The Lead Plaintiff in this action is Thomas P. DiNapoli, Comptroller of the State of New York, as Administrative Head of the New York State and Local Retirement System, and as Trustee of the New York State Common Retirement Fund. Lead Plaintiff brings these claims on behalf of itself and all other similarly situated persons or entities who purchased or otherwise acquired CrowdStrike common stock between September 20, 2022, and July 30, 2024, inclusive ("the Class Period"), and were damaged thereby (collectively, "the Class"). Hereinafter, the Court will refer to the class-action plaintiffs as "Plaintiffs." Plaintiffs later filed a consolidated class action complaint bringing claims under Section 10(b) of the Exchange Act and Rule 10b-5 against all Defendants, as well as claims under Section 20(a) of the Exchange Act against Defendants Kurtz and Sentonas. (*Id.* at 92, 94).

CrowdStrike sells the Falcon cybersecurity platform, which CrowdStrike reportedly emphasized is updated automatically and remotely, without customers needing to reboot or manage updates. (*Id.* at 13). According to Plaintiffs' Complaint, CrowdStrike "amassed a customer base that included the U.S. federal government, 43 out of 50 state governments, and more than half of the Fortune 500 companies" through Defendants' representations regarding the company's robust testing and quality assurance processes. (*Id.* at 7). Plaintiffs claim these remote updates, called "Rapid Response Content updates," were "central" to CrowdStrike's pitch to investors, as the Rapid Response updates "made its Falcon cybersecurity threat detection software better than its competitors." (*Id.* at 13). Falcon operates at the "kernel level" of a computer, i.e., at "the heart of a computer's operating system." (*Id.* at 15). According to Plaintiffs, kernel-level software comes with "heightened risk and increased responsibility" as compared to user-level software. (*Id.* at 15–16).

Plaintiffs allege that Defendants "specifically and repeatedly highlighted their testing of CrowdStrike's software" and provide the Court with a number of statements from Defendants that Plaintiffs claim were misleading or false. (*Id.* at 13, 26–28). CrowdStrike allegedly claimed that its "software development methodology . . . allows for rapid, frequent, and reliable code updates." (*Id.* at 13). Defendant Kurtz allegedly told investors on the first day of the Class Period, September 20, 2022, that "[t]esting and validation is really important" and stressed that "[w]e test more than anyone else." (*Id.* at 26). Similarly, during a quarterly earnings call in August 2023, Defendant Kurtz told investors that CrowdStrike's testing prevents "insecure code . . . being put into the [update] pipeline." (*Id.* at 26). In another public representation during the Class Period, CrowdStrike represented that it tests its Falcon software updates "in non-production environments" before "roll[ing] them out." (*Id.* at 26). In April 2023, Defendant Sentonas stated that Falcon doesn't cause computers to blue screen (i.e., crash),[2] which he acknowledged is "one of the most important things" to CrowdStrike's customers. (*Id.* at 27). Defendants also told investors that it had a "quality assurance team." (*Id.* at 28). Plaintiffs allege that securities analysts rated CrowdStrike's stock as "BUY" in part due to CrowdStrike's "representations about its stable and secure software updates." (*Id.* at 7). At the beginning of the Class Period, CrowdStrike's stock price was $174 per share; the stock price more than doubled to a Class Period high of $392 per share. (*Id.*).

Plaintiffs allege that CrowdStrike's website also contained multiple false or misleading statements about its testing. CrowdStrike's website represented that the company "always [does] canary deployments of new services before rolling out changes to the entire fleet," i.e., it does phased rollouts to ensure that if there is a problem with a new update, they can catch it before the update has gone to all of its customers. (*Id.* at 27, 36). Plaintiffs plead that canary deployments are an "industry standard." (*Id.* at 36). On July 4, 2024, a page on CrowdStrike's website was posted that explained its adherence to "continuous integration and continuous delivery (CI/CD)," which is a "software development methodology that allows for rapid, frequent, and reliable code updates." (*Id.*

[2] A blue screen on a computer running Microsoft Windows refers to the computer crashing and becoming inoperable. (Compl., Dkt. 41, at 16).

at 77). According to Plaintiffs, the page on CI/CD states that CrowdStrike deployed software updates to a "staging environment that closely resembles the production environment" for "[f]urther testing." (*Id.*).

In addition, Defendants represented that CrowdStrike adheres to the "stringent requirements" of the Federal Risk and Authorization Management Program ("FedRAMP"), which "standardizes how non-government entities implement security controls to ensure they align with government standards," and adheres to the U.S. Department of Defense's ("DoD") compliance requirements.[3] (*Id.* at 29). The website specifically stated that the company complies with FedRAMP and with DoD Impact Level 4.[4] (*Id.* at 76). According to Plaintiffs:

> FedRAMP and DoD expressly mandate that software companies like CrowdStrike: (i) test new updates in a preproduction environment that replicates the production environment such software will run on when released to customers, (ii) utilize a phased rollout process to ensure that errors are identified in a small number of production environments before updates are released to the vast majority of customers, and (iii) maintain quality assurance staff distinct from software developers to conduct such testing and in accordance with standardized test plans. The federal government also requires companies seeking FedRAMP or DoD authorization to explicitly certify that they meet the above requirements.

(*Id.* at 30). Plaintiffs plead that the above-described representations by CrowdStrike that they claim were false or misleading were material to investors. (*Id.* at 78–79).

The parties do not appear to dispute that on July 19, 2024, CrowdStrike released an update or updates that triggered an error, causing some computers running Microsoft Windows to "blue screen." (*Id.* at 8; Mot. to Dismiss, Dkt. 47, at 9). According to Plaintiffs, approximately 8.5 million computers running Microsoft Windows "simultaneously and immediately" blue screened and were

[3] FedRAMP's and DoD's requirements incorporate the industry standards for information security and cybersecurity set by the National Institute of Standards and Technology ("NIST"). (Compl., Dkt. 41, at 6).

[4] Plaintiffs assert that investors in CrowdStrike valued Defendants' representation that CrowdStrike meets these federal government requirements, as CrowdStrike needed to comply with those standards to "win and maintain business from the federal government (one of its largest customers)." (*Id.* at 28). For example, financial analysts at two companies allegedly cited CrowdStrike's compliance with FedRAMP and DoD requirements as a reason to purchase CrowdStrike stock. (*Id.* at 30–31).

"tak[en] . . . out of commission." (Compl., Dkt. 41, at 8, 49). The widespread outages caused "global disruption, with airlines, public hospitals, financial services, and police departments brought to a complete standstill." (*Id.* at 8). Certain commentators described this incident as "the largest IT outage in history." (*Id.* at 42). As a result of the outages, CrowdStrike's stock value plummeted "by nearly 32%—the largest stock price decline in CrowdStrike's history as a publicly traded company," leading to the present consolidated class action.[5] (Compl., Dkt. 41, at 9–10).

On the day of the outage, Kurtz appeared on NBC's Today Show to apologize for the outage. (*Id.* at 42). He explained that the "system was sent an update and that update had a software bug in it and caused an issue with the Microsoft operating system." (*Id.*). CrowdStrike subsequently published a formal statement admitting that the outage was "caused by a defect found in a Falcon content update for Windows hosts." (*Id.*). On July 24, 2024, CrowdStrike released a Preliminary Post Incident Review ("PIR") that, according to Plaintiffs, "confirmed that CrowdStrike was *not* conducting necessary testing despite years of representations to the contrary." (*Id.* at 50). The PIR allegedly also acknowledged that, had CrowdStrike conducted the tests it represented it used, the faulty update would have been caught prior to its release. (*Id.*). CrowdStrike committed itself to "adopting pre-production environment testing and phased rollouts for all future" Rapid Response Content updates. (*Id.* at 50–51). On August 10, 2024, Sentonas attended a hacking conference, where he accepted the "Most Epic Fail" award on behalf of CrowdStrike for causing the global IT outage; Sentonas reportedly stated when accepting the award that it is "super important to own it when you do things horribly wrong, which we did in this case . . . . [We] got this wrong." (*Id.* at 53). Plaintiffs allege that on September 24, 2024, a CrowdStrike executive, Adam Meyers, testified before the House Cybersecurity and Infrastructure Protection Subcommittee that CrowdStrike did not test software updates in a pre-production environment and did not conduct phased rollouts of such

[5] Specifically, CrowdStrike stock fell nearly 32% between July 19, 2024, and July 30, 2024. (*Id.* at 50).

updates. (*Id.* at 53–54). Meyers further stated that CrowdStrike would now begin to conduct such tests and phased rollouts to "avert future, similar incidents." (*Id.* at 53–54).

Plaintiffs plead that industry experts harshly criticized Defendants' "admitted" failure to follow "industry-standard practices." (*Id.* at 43–48, 50). A computer science professor opined that CrowdStrike's process for pushing out software updates was "very irresponsible" and did not align with the process followed by "lots of other companies that are using industry standards" to update their software. (*Id.* at 43). One cybersecurity expert stated that the outage was caused by "intentional architectural, engineering, and [quality assurance] decisions" made by CrowdStrike. (*Id.* at 43). Another expert argued that this incident made clear CrowdStrike's Rapid Response updates are not thoroughly tested before being deployed, which he called a "serious process design failure for their product Quality Assurance." (*Id.* at 45). Industry experts also noted that CrowdStrike's failure to properly test its Rapid Response updates may violate the NIST industry standards that are incorporated into the FedRAMP and DoD requirements. (*Id.* at 46). Finally, industry experts noted the outage's similarity with an outage in 2010 caused by McAfee, another cybersecurity company. (*Id.* at 47). Defendants Kurtz and Sentonas had been Chief Technology Officers of McAfee at the time of the 2010 outage, which was also caused by a faulty update that had not been released in phases. (*Id.* at 47–48).

Regarding scienter, Plaintiffs allege that Defendants knew, or at a minimum were severely reckless in not knowing, that their statements to investors regarding CrowdStrike's testing of its software updates were false or misleading by omission. (*Id.* at 55). Plaintiffs support their allegation of scienter by pleading that Falcon was CrowdStrike's only product, meaning Defendants would know (or were severely reckless in not knowing) that it was not being properly tested and rolled out; that Defendants specifically and repeatedly touted its testing processes; that Defendants told investors Falcon does not cause blue screens; that Defendants Kurtz and Sentonas claimed to have "learned their lesson" at McAfee about insufficient quality assurance processes for software updates; that Defendants had claimed before and during the Class Period that CrowdStrike does pre-production testing and phased rollouts, meaning Defendants knew the industry standards; that Defendants represented they had a "quality assurance team"—the absence of such would be obvious to Defendants; that Defendants were required to sign sworn verifications that CrowdStrike's software complied with NIST requirements; that CrowdStrike employees had raised concerns to Defendants regarding the focus on speed over quality; and that CrowdStrike had previously released faulty updates that had not been properly tested, causing certain systems to crash. (*Id.* at 55–64). Regarding Defendant Kurtz specifically, Plaintiffs point out that he published a book on cybersecurity that acknowledges the risk of kernel-level software and discusses the need for developers doing "[r]apid patch deployment" to "be sure to test new patches for compatibility with the environment and applications." (*Id.* at 65). Plaintiffs also claim that Defendants admitting "we got this wrong" and never denying that they knew of the deficient testing practices strengthens the scienter inference. (*Id.* at 66).

Finally, Plaintiffs plead that Defendants' misstatements and omissions alleged in the complaint "artificially inflated the price of CrowdStrike's stock during the Class period" and that the "artificial inflation was removed when the conditions and risks misstated and omitted by Defendants and/or the materialization of the risks concealed by Defendants' misleading statements and omissions were revealed to the market." (*Id.* at 81). Analysts at various investment firms "downgraded" the company's stock after the outage. (*Id.* at 84). For example, HSBC downgraded CrowdStrike from "Buy" to "Hold," citing "new risks," and analysts at BTIG downgraded CrowdStrike to "Neutral" due to "concern[] over near-term demand trends stemming from an outage created by a [CrowdStrike] software update that disrupted businesses globally." (*Id.* at 84–85). Plaintiffs assert that it was foreseeable that Defendants' materially false and misleading statements and omissions would artificially inflate the price of CrowdStrike securities and that "the decline in CrowdStrike's stock price was a direct and proximate result of the truth being revealed to investors and the market." (*Id.* at 87).

II. LEGAL STANDARD

Pursuant to Rule 12(b)(6), a court may dismiss a complaint for "failure to state a claim upon which relief can be granted." Fed. R. Civ. P. 12(b)(6). In deciding a 12(b)(6) motion, a "court accepts 'all well-pleaded facts as true, viewing them in the light most favorable to the plaintiff.'" *In re Katrina Canal Breaches Litig.*, 495 F.3d 191, 205 (5th Cir. 2007) (quoting *Martin K. Eby Constr. Co. v. Dall. Area Rapid Transit*, 369 F.3d 464, 467 (5th Cir. 2004)). A court ruling on a 12(b)(6) motion may rely on the complaint, its proper attachments, "documents incorporated into the complaint by reference, and matters of which a court may take judicial notice." *Dorsey v. Portfolio Equities, Inc.,* 540 F.3d 333, 338 (5th Cir. 2008) (citations and internal quotation marks omitted). A court may also consider documents that a defendant attaches to a motion to dismiss "if they are referred to in the plaintiff's complaint and are central to her claim." *Causey v. Sewell Cadillac-Chevrolet, Inc.*, 394 F.3d 285, 288 (5th Cir. 2004). But because the court reviews only the well-pleaded facts in the complaint, it may not consider new factual allegations made outside the complaint. *Dorsey,* 540 F.3d at 338. "[A] motion to dismiss under 12(b)(6) 'is viewed with disfavor and is rarely granted.'" *Turner v. Pleasant*, 663 F.3d 770, 775 (5th Cir. 2011) (quoting *Harrington v. State Farm Fire & Cas. Co.*, 563 F.3d 141, 147 (5th Cir. 2009)).

Fraud claims have a heightened pleading standard, as they must be plead "with particularity." Fed. R. Civ. P. 9(b). Accordingly, plaintiffs must "state all allegations of fraud with particularity by identifying the 'time, place, and contents of the false representations, as well as the identity of the person making the misrepresentation and what that person obtained thereby.'" *Owens v. Jastrow*, 789 F.3d 529, 535 (5th Cir. 2015) (quoting *Tuchman v. DSC Commc'ns Corp.*, 14 F.3d 1061 (5th Cir. 1994)).

III. DISCUSSION

Defendants move to dismiss Plaintiffs' Complaint for failure to state a claim. (Mot. to Dismiss, Dkt. 47, at 6). Section 10 of the Exchange Act states:

> It shall be unlawful for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce or of the mails, or of any facility of any national securities exchange . . .
>
> (b) To use or employ, in connection with the purchase or sale of any security registered on a national securities exchange or any security not so registered, or any securities-based swap agreement any manipulative or deceptive device or contrivance in contravention of such rules and regulations as the Commission may prescribe as necessary or appropriate in the public interest or for the protection of investors . . . .

15 U.S.C. § 78j(b). Rule 10b-5 states:

> It shall be unlawful for any person, directly or indirectly, by the 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.

17 C.F.R. § 240.10b-5.

To state a viable securities fraud claim under Section 10(b) and Rule 10b-5, Plaintiffs must allege that: (1) Defendants made a misrepresentation or omission relating to the purchase or sale of a security; (2) such representation or omission related to a material fact; (3) the representation or omission was made with scienter;[6] (4) Plaintiffs acted in reliance on Defendants' representation or omission; and (5) the representation or omission proximately caused Plaintiffs' losses. *Alaska Elec.*

[6] Scienter is "a mental state embracing intent to deceive, manipulate, or defraud." *Goldstein v. MCI WorldCom*, 340 F.3d 238, 245 (5th Cir. 2003) (quoting *Ernst & Ernst v. Hochfelder*, 425 U.S. 185, 193 n.12 (1976)).

Pension Fund v. Flotek Indus., Inc., 915 F.3d 975, 981 (5th Cir. 2019). These claims are subject to the pleading standard set forth by Federal Rule of Civil Procedure 9(b), as described in Section II, *supra*, as well as the pleading requirements mandated by the Private Securities Litigation Reform Act ("PSLRA"). *Spitzberg v. Hous. Am. Energy Corp.*, 758 F.3d 676, 683 (5th Cir. 2014). The PSLRA requires that allegations of securities fraud "[a]t a minimum . . . incorporate[] the 'who, what, when, where, and how' requirements of" Federal Rule of Civil Procedure 9(b). *Owens*, 789 F.3d at 535 (citing *ABC Arbitrage Plaintiffs Grp. v. Tchuruk*, 291 F.3d 336, 349–50 (5th Cir. 2002)). Specifically, for claims brought under the PSLRA to survive a motion to dismiss, the plaintiff must: "(1) specify each statement alleged to have been misleading; (2) identify the speaker; (3) state when and where the statement was made; (4) plead with particularity the contents of the false representation; (5) plead with particularity what the person making the misrepresentation obtained thereby; and (6) explain the reason or reasons why the statement is misleading, *i.e.*, why the statement is fraudulent." *In re BP p.l.c. Sec. Litig.*, 843 F. Supp. 2d 712, 746 (S.D. Tex. 2012) (citing *ABC Arbitrage Plaintiffs Grp.*, 291 F.3d at 350).

Defendants argue that Plaintiffs' Section 10(b) claim should be dismissed because they have failed to sufficiently plead any actionable misstatements or omissions and have failed to sufficiently plead scienter. (Mot. to Dismiss, Dkt. 47, at 13, 32). Accordingly, Defendants also argue that Plaintiffs' Section 20(a) claim should be dismissed because Plaintiffs have failed to state a claim for a primary violation of Section 10(b). (*Id.* at 40).

A. Defendants' Request for Judicial Notice or Incorporation-by-Reference

Defendants attach twenty-eight exhibits to their Motion to Dismiss. In a footnote, Defendants claim that these exhibits "are properly before the Court because they are each subject to judicial notice, are incorporated by reference, or both." (*Id.* at 9 n.4). Plaintiffs filed an Opposition to Defendants' Request for Judicial Notice or Incorporation-by-Reference. (Opp. to Judicial Not., Dkt.

49). Plaintiffs argue that Defendants' footnote is conclusory, that Defendants do not distinguish which documents fall into which category or explain the basis on which the Court should consider these documents, and that Defendants mischaracterize their own exhibits. (*Id.* at 5–6).

The Supreme Court has held that, when ruling on a motion to dismiss a § 10(b) action for failure to state a claim, "courts **must** consider the complaint in its entirety, as well as other sources courts ordinarily examine when ruling on Rule 12(b)(6) motions to dismiss, in particular, documents incorporated into the complaint by reference, and matters of which a court may take judicial notice." *Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 322 (2007) (emphasis added). The Court will therefore consider documents incorporated into Plaintiffs' Complaint by reference and documents of which the Court may properly take judicial notice, including SEC filings.[7] The Court will therefore consider Defendants' Exhibits A, B, C, D, E, F, G, I, J, K, N, O, P, Q, R, S, T, U, V, W, X, Y, Z, AA, and BB attached to its motion to dismiss. Nonetheless, the Court is mindful that, "as with any motion to dismiss for failure to plead a claim on which relief can be granted, [the Court must] accept all factual allegations in the complaint as true"; the judicially noticed documents are therefore considered not for the truth of their contents, but for what statements they contain. *Tellabs*, 551 U.S. at 322; *Linenweber v. S.W. Airlines Co.*, 693 F. Supp. 3d 661, 674 (N.D. Tex. 2023). The Court will not consider or take judicial notice of Defendants' Exhibits H, L, and M, which are

[7] The Fifth Circuit has held that, when deciding on a motion to dismiss a claim for securities fraud on the pleadings, a court may take judicial notice of SEC filings "to the extent that they are 'considered only for the purpose of determining what statements the documents contain, not to prove the truth of the documents' contents.'" *Petrobras Am., Inc. v. Samsung Heavy Industries Co., Ltd.*, 9 F.4th 247, 255 (5th Cir. 2021) (quoting *Lovelace v. Software Spectrum, Inc.*, 78 F.3d 1015, 1018 (5th Cir. 1996)). The Court may also take judicial notice of governmental websites. *See Kitty Hawk Aircargo, Inc. v. Chao*, 418 F.3d 453, 457 (5th Cir. 2005) (taking judicial notice of information published on the National Mediation Board's website); *Coleman v. Dretke*, 409 F.3d 665, 667 (5th Cir. 2005) (per curiam) (taking judicial notice of a Texas agency's website).

pages on CrowdStrike's website not referenced in Plaintiffs' Complaint and which the Court does not deem relevant to its analysis.[8]

B. Misstatements and Omissions

Defendants argue that the alleged misstatements and omissions relied upon by Plaintiffs are "rampant mischaracterizations of Defendants' statements that take them out of their context and distort them beyond recognition." (Mot. to Dismiss, Dkt. 47, at 13). They contend that, though well-pled allegations are generally assumed true, Plaintiffs are not entitled to such a presumption if the allegations contradict facts subject to judicial notice or incorporated by reference. (*Id.*). The Court agrees that it cannot credit a plaintiff's allegations contradicted by documents that the Court may consider at this stage. *See U.S. ex rel. Riley v. St. Luke's Episcopal Hosp.*, 355 F.3d 370, 377 (5th Cir. 2004) (citing *Simmons v. Peavy-Welsh Lumber Co.*, 113 F.2d 812, 813 (5th Cir. 1940)) ("If such an allegation is contradicted by the contents of an exhibit attached to the pleading, then indeed the exhibit and not the allegation controls."); *Carter v. Target Corp.*, 541 F. App'x 413, 416–17 (5th Cir. 2013) (per curiam) (refusing to accept as true factual allegations that were contradicted by the plaintiff's EEOC charging documents, which were referenced in the complaint and attached to the defendant's motion to dismiss); *Linenweber*, 693 F. Supp. 3d at 680–81 (reviewing alleged misstatements in their context in a Section 10(b) case by considering documents referenced in the complaint and attached to the motion to dismiss). With this rule in mind, the Court will analyze in turn each of the misrepresentations or omissions alleged by Plaintiffs. For clarity, the Court will organize the alleged misrepresentations or omissions as Defendants did in their Chart of Alleged Misstatements, (Dkt. 47-1).

[8] *See U.S. ex rel. Branch Consultants, L.L.C. v. Allstate Ins. Co.*, 668 F. Supp. 2d 780, 789 (E.D. La. 2009) ("Courts may not take judicial notice of irrelevant facts."); *Austin's Nat. Frozen Pops, Inc. v. Jonny Pops, LLC*, No. 1:24-CV-716-RP, 2025 WL 888560, at *3 (W.D. Tex. Mar. 13, 2025) (acknowledging that use of judicial notice should be "sparing" at the motion-to-dismiss stage).

1. Statements About a "Quality Assurance Team"

Plaintiffs allege that quality assurance teams are a "necessary and important aspect of software development," as they "conduct the necessary tests of software updates and ensure that [the updates] do not crash customers' computers upon release." (Compl., Dkt. 41, at 20–21). Plaintiffs plead that in CrowdStrike's annual Proxy Statements, Defendants "touted CrowdStrike's 'quality assurance team,' which was supposedly 'trained and equipped to assist with testing.'" (*Id.* at 6, 28). According to former CrowdStrike employees, however, CrowdStrike in fact "lacked a quality assurance team or even test plans for its software updates." (*Id.* at 32, 34). Plaintiffs thus claim it "was false or, at minimum, misleading for CrowdStrike to assure investors that CrowdStrike maintained a 'quality assurance team' that 'assist[ed] with testing' software updates." (*Id.* at 75).

Defendants argue in their Motion to Dismiss that Plaintiffs have "strip[ped]" these statements about CrowdStrike having a quality assurance team out of their context. (Mot. to Dismiss, Dkt. 47, at 14–15). The statement quoted by Plaintiffs in their Complaint—that CrowdStrike has a "quality assurance team . . . trained and equipped to assist with testing"—is from the "Accessibility" section of CrowdStrike's 2023 and 2024 Proxy Statements. (2023 Proxy Statement, Dkt. 47-10, at 22; 2024 Proxy Statement, Dkt. 47-11, at 22). The full paragraph up until that sentence is:

> CrowdStrike takes accessibility of its products very seriously, with dedicated accessibility specialists on staff as part of a program of continuous education on accessible design and engineering for those working on our customer-facing user-interfaces. In particular, we focus on screen reader compatibility for visually impaired users and color/contrast configurability to optimize our experience for various classes of color-blindness. **Our quality assurance team is also trained and equipped to assist with testing for accessibility** and we work with external accessibility auditors to help identify any deficiencies.

(2023 Proxy Statement, Dkt. 47-10, at 22) (emphasis added).[9] Defendants contend that Plaintiffs' allegations regarding CrowdStrike's lack of a quality assurance team for software or content updates do not falsify CrowdStrike's statement that it has a quality assurance team for accessibility. (Mot. to Dismiss, Dkt. 47, at 15).

Plaintiffs respond that, though the statement above was made in the context of describing CrowdStrike's accessibility efforts, CrowdStrike never told investors "that it *only* had a quality assurance team for accessibility testing." (Pls.' Resp., Dkt. 48, at 34). Rather, the Proxy Statement says that the company's quality assurance team is "*also* trained and equipped to assist with testing for accessibility," which Plaintiffs argue "does not state or imply that CrowdStrike's 'quality assurance team' was limited exclusively to 'testing for accessibility.'" (*Id.* at 34) (emphasis added by Plaintiffs).

The Court agrees with Defendants that the statements pointed to by Plaintiffs are "neither false nor misleading when considered in the context from which Plaintiffs removed them." *See Linenweber*, 693 F. Supp. 3d at 680. CrowdStrike's 2023 and 2024 Proxy Statements are the **only** instances Plaintiffs point to where CrowdStrike represented it had a "quality assurance team." Plaintiffs' assertion in their Complaint that it "was false or, at minimum, misleading for CrowdStrike to assure investors that CrowdStrike maintained a 'quality assurance team' *that 'assist[ed] with testing' software updates,*" (*Id.* at 75) (emphasis added), is **borderline sanctionable**, as CrowdStrike **never** told investors that it had a quality assurance team that assisted with software updates. *See Thornton v. Micrografx, Inc.*, 878 F. Supp. 931, 936 (N.D. Tex. 1995) ("The Court concludes that if anyone is being misleading, it is the Plaintiffs."). When read in context, no reasonable investor would have assumed purely from a single sentence in the Accessibility section of CrowdStrike's 2023 and 2024

[9] Though there are slight differences in the wording in CrowdStrike's 2024 Proxy Statement, (Dkt. 47-11), the wording is very similar.

Proxy Statements that CrowdStrike had a quality assurance team that tested software updates.[10] *See Omnicare, Inc. v. Laborers Dist. Council Constr. Indus. Pension Fund*, 575 U.S. 175, 190 (2015) ("[A]n investor reads each statement within such a document, whether of fact or of opinion, in light of all its surrounding text, including hedges, disclaimers, and apparently conflicting information.").

Moreover, even if CrowdStrike's reference to a "quality assurance team" was misleading, the Court finds that Plaintiffs have not plausibly alleged that this statement was material. "To prevail on a § 10(b) claim, a plaintiff must show that the defendant made a statement that was 'misleading as to a *material* fact.'" *Matrixx Initiatives, Inc. v. Siracusano*, 563 U.S. 27, 38 (2011) (emphasis in original) (quoting *Basic Inc. v. Levinson*, 485 U.S. 224, 238 (1988)). A "statement or omitted fact is 'material' if there is a substantial likelihood that a reasonable investor would consider the information important in making a decision to invest." *ABC Arbitrage Plaintiffs Grp.*, 291 F.3d at 359 (citing *R&W Technical Servs. Ltd. v. Commodity Futures Trading Comm'n*, 205 F.3d 165, 169 (5th Cir. 2000)). Omitted facts make a statement material only when there is "a substantial likelihood that the disclosure of the omitted fact would have been viewed by the reasonable investor as having significantly altered the 'total mix' of information made available." *Matrixx Initiatives*, 563 U.S. at 38 (quoting *Basic*, 485 U.S. at 231–32)). A court's materiality analysis "requires consideration of the source, content, and context" of the statement. *Id.* at 43. Though the materiality analysis is "usually left for the jury," courts may find statements to be immaterial as a matter of law on a motion to dismiss. *ABC Arbitrage Plaintiffs Grp.*, 291 F.3d at 359.

Plaintiffs plead that Defendants "touted CrowdStrike's 'quality assurance team,' which was supposedly 'trained and equipped to assist with testing.'" (Compl., Dkt. 41, at 6). The assertion that

[10] Defendants also claim that the Court must discount Plaintiffs' allegations regarding CrowdStrike's lack of a quality assurance team, as the allegations come only from confidential sources. (Mot. to Dismiss, Dkt. 47, at 16–17). Because the Court has already found that the statements about a quality assurance team were not misleading in their context, the Court does not reach this argument.

CrowdStrike's use of the phrase "quality assurance team" in the singular context of testing *for accessibility* on page 18 of its 2023 and 2024 Proxy Statements qualifies as "tout[ing]" is unwarranted. When considering the "source, content, and context" of the statement, *see Matrixx Initiatives*, 563 U.S. at 43, no reasonable investor would read the sentence, "Our quality assurance team is also trained and equipped to assist with testing for accessibility, and we work with external accessibility auditors to help identify any deficiencies," interpret the sentence as referring to a quality assurance team for testing its software for defects, and then use that information in their investment decision. Thus, Plaintiffs have failed to plausibly allege that CrowdStrike's 2023 and 2024 Proxy Statements included a material misrepresentation regarding it having a "quality assurance team that 'assist[ed] with testing' software updates." (*See* Compl., Dkt. 41, at 75).

2. Statements About Product Usage

Defendants argue that six of the misstatements or omissions alleged by Plaintiffs were statements about how CrowdStrike software could be used by its customers, rather than about CrowdStrike's own software development processes. (Mot. to Dismiss, Dkt. 47, at 17–21). First, Plaintiffs allege that "Defendants assured investors on CrowdStrike's website that it adhered to 'continuous integration and continuous delivery (CI/CD),' which 'is a software development methodology that allows for rapid, frequent, and reliable code updates.'"[11] (Compl., Dkt. 41, at 77). Plaintiffs further claim that CrowdStrike stated on this webpage that it "deployed software updates to a 'staging environment that closely resembles the production environment" for "[f]urther testing," including "[p]erformance testing, security testing, user acceptance test (UAT), and other testing . . . ." (*Id.*). Plaintiffs allege that these statements were false or misleading because

[11] The webpage referred to by Plaintiffs is attached to Defendants' Motion to Dismiss as Exhibit I, (Dkt. 47-13).

CrowdStrike did not test its software updates in a "staging environment that closely resembles the production environment" for "further testing," which led to the July 2024 outage. (*Id.* at 77–78).

Defendants argue in their Motion to Dismiss that the webpage Plaintiffs cite to about CI/CD never represents that CrowdStrike uses CI/CD. Rather, Defendants assert that the article's purpose is to educate customers and potential customers about CI/CD; it never claims that CrowdStrike adheres to this methodology. Plaintiffs respond that, even if Defendants' interpretation of the article is true, they have raised a fact dispute regarding whether a reasonable investor "would understand that statement to assert that CrowdStrike practiced what it preached." (Pls.' Resp., Dkt. 48, at 28).

The Court agrees with Defendants. The webpage is unquestionably an educational article in a series called "Cybersecurity 101"; there is **no** indication in the article that CrowdStrike uses CI/CD. (CI/CD Article, Dkt. 47-13). For example, the article states, "Though CI/CD can greatly enhance the efficiency and speed of *your* pipeline, it's important to ensure that *your* automation solves problems rather than introducing them." (*Id.*) (emphasis added). In context, *see Omnicare*, 575 U.S. at 190, no reasonable investor would be misled to believe this article means CrowdStrike uses the CI/CD methodology.[12]

Second and third, Plaintiffs allege that Kurtz made two statements about Falcon's capabilities related to "insecure code." Plaintiffs plead that during an Investor Briefing, Kurtz "highlighted [CrowdStrike's] ability 'to understand if insecure code is being put into the CI/CD pipeline." (Compl., Dkt. 41, at 70). Additionally, Plaintiffs assert that while speaking at a conference, Kurtz similarly "highlighted [CrowdStrike's] purported 'ability to help make sure that code is secure,

[12] Nor would the Court expect a reasonable investor to rely upon any "Cybersecurity 101" article written by a CrowdStrike software engineer to make an investment decision. *See Basic Inc.*, 485 U.S. at 234 (citing *TSC Industries, Inc. v. Northway Inc.*, 426 U.S. 438, 448–49 (1976)) ("The role of the materiality requirement is . . . to filter out essentially useless information that a reasonable investor would not consider significant . . . .").

that it's deployed and that it's run in a secure environment.'" (*Id.* at 70–71). They argue that these two statements were false or misleading because Kurtz omitted that CrowdStrike did not test its software updates for "insecure code," did not have a quality assurance team for software updates, and prioritized speed over quality control. (*Id.*)

Defendants contend that Plaintiffs have again taken these statements out of context. According to Defendants, these two statements made by Kurtz were about how Falcon protects customers who are updating their own product code, "i.e., non-CrowdStrike" code. (Mot. to Dismiss, Dkt. 47, at 19). Plaintiffs again respond that they have raised a fact issue as to whether a reasonable investor would have understood these statements to also refer to CrowdStrike's own processes. (Pls.' Resp., Dkt. 48, at 28). The Court agrees with Defendants that these statements, when read in context, (Dkts. 47-14, 47-15), are surely about *non*-CrowdStrike code.[13] The Court therefore finds that Plaintiffs have failed to adequately allege that these statements regarding CrowdStrike's coding processes were false or misleading. *See Lormand v. US Unwired, Inc.*, 565 F.3d 228, 239 (5th Cir. 2009) ("[T]he PSLRA requires a plaintiff to identify each allegedly misleading statement with particularity and explain why it is misleading.").

Fourth and fifth, Plaintiffs allege that Kurtz made two misleading or false statements about CrowdStrike's software preventing blue screens, i.e., crashes. Kurtz purportedly stated in a November 2023 earnings call: "We've got many, many airlines that use our technology. They don't want to send out an IT person to go fix a kiosk that has a Microsoft blue screen. So what can they do? They can use Falcon for IT." (Compl., Dkt. 41, at 71). Kurtz also allegedly claimed in an interview, "We have airlines that you know when the kiosk is kind of blue screened, you know

[13] The Court also notes its skepticism of Plaintiffs' proffered interpretation of the term "insecure." In light of CrowdStrike being a cybersecurity company, it is far more plausible that when CrowdStrike refers to customers' "insecure code," it is referring to code that literally makes the customers' systems less secure—i.e., makes them susceptible to data breaches—rather than referring to code containing bugs.

when you go through the airport and you see the Microsoft blue screen, they actually, yeah well they actually use our technology to fix it." (*Id.* at 72). According to Plaintiffs, these two statements were misleading or false because Kurtz omitted that CrowdStrike "did not test its software updates in a pre-production environment, contrary to basic industry standards . . . which directly exposed its user-endpoints[14] to bluescreening." (*Id.*).

Defendants argue in their Motion to Dismiss that Plaintiffs are distorting what Kurtz said. Instead, they contend that he was explaining Falcon for IT allows blue screens on airline kiosks to be fixed remotely, rather than needing a person to physically travel to the kiosk to reboot it. Plaintiffs respond that by "touting that Falcon 'fixes' blue screens when Falcon actually *causes* blue screens with untested updates, Kurtz misled investors." (Pls.' Resp., Dkt. 48, at 22). This argument by Plaintiffs fails. Even accepting Plaintiffs' contention that Falcon can cause a computer to crash, Kurtz's statements that airlines can use Falcon to remotely fix a crashed computer are not falsified nor misleading. It can be true that the same software can both cause a blue screen and then be used to fix that blue screen. No reasonable investor would hear Kurtz's statement about a feature of Falcon for IT—a statement unrelated to CrowdStrike's software development process—and assume it means CrowdStrike's software would never cause crashes. Moreover, Plaintiffs do not allege that Falcon for IT is *not* used by customers to remotely reboot their systems. Plaintiffs have therefore failed to sufficiently plead that these statements made by Kurtz were false or misleading. *See Lormand*, 565 F.3d at 239.

Sixth, Plaintiffs allege that CrowdStrike's Vice President of Product Management, Sanjay Chaudhary, made a false statement on behalf of CrowdStrike on April 18, 2024, when he stated that

[14] Defendants represent that user-endpoints include "laptops, desktops, and servers." (Mot. to Dismiss, Dkt. 47, at 8).

"our focus has always been an API-first approach.[15] We don't want you to just go on the UI and build one detection. Rather, programmatically build hundreds of detections, test those in non-production environments, and roll them out." (Compl., Dkt. 41, at 73; Chaudhary Transcript, Dkt. 47-20, at 12). Plaintiffs plead that this statement was false or misleading because CrowdStrike did not test its updates in non-production environments.[16] (Compl., Dkt. 41, at 73).

Defendants reiterate that Plaintiffs have distorted CrowdStrike's words. They assert that Chaudhary was not speaking about CrowdStrike's own updates; rather, he was referring to customers building their own updates using Falcon's API. (Mot. to Dismiss, Dkt. 47, at 21). They emphasize the beginning of Chaudhary's statement: "We don't want *you* to . . . ." (*Id.*). Plaintiffs respond that "Defendants again impermissibly ask the Court to take them at their word that no reasonable investor understood [Chaudhary] also to refer to CrowdStrike's own update testing." (Pls.' Resp., Dkt. 48, at 28).

The Court agrees with Defendants that, in context, no reasonable investor would understand Chaudhary as speaking about CrowdStrike's own software; he said nothing about CrowdStrike's software development process. Plus, any allegations made by Plaintiffs about CrowdStrike's failure to test its own updates do not falsify Chaudhary's statement that CrowdStrike's customers are advised to test in non-production environments. *See Lormand*, 565 F.3d at 239. And no reasonable investor would assume in this context that, because Chaudhary did not state that CrowdStrike does not do such testing, CrowdStrike impliedly must do such testing. Plaintiffs therefore have not

[15] "API" stands for "application programming interface," which Defendants represent is "a tool that helps software developers build their own solutions." (Mot. to Dismiss, Dkt. 47, at 21).

[16] Plaintiffs also plead that this statement is misleading because CrowdStrike "did not 'programmatically' 'roll out' its software updates." (Compl., Dkt. 41, at 73). This is a severe manipulation of what CrowdStrike's Vice President said. He never used the phrase "programmatically roll out" updates, even when referring to what its customers should do. Rather, he told customers to "programmatically build hundreds of detections, test those in non-production environments, and roll them out" (*Id.*). The Court cautions Plaintiffs' counsel against distorting quotes in this manner.

sufficiently pleaded that the six statements about customers using CrowdStrike software were misleading or false.

3. Statements About Testing and/or Software Updates

Next, there are five statements related to CrowdStrike's testing and/or software updates that Plaintiffs claim were false or misleading. Defendants argue that, as a threshold matter, Plaintiffs are incorrectly conflating software and code with Rapid Response Content. (Mot. to Dismiss, Dkt. 47, at 21–22). According to Defendants, Rapid Response Content is not software or code. (*Id.*). Defendants point to CrowdStrike executive Adam Meyers's sworn testimony before Congress, which was referenced by Plaintiffs in their Complaint; he testified, in response to a question that characterized the incident as being caused by a software update, that "the content update was not code. This was threat information that was being provided to the sensor." (Meyers Testimony, Dkt. 47-21, at 19). Plaintiffs argue that whether Rapid Response Content is software or code is a "highly fact-intensive assertion" and that it would be improper for the Court to determine at the pleading stage how reasonable investors understood these updates. (Pls.' Resp., Dkt. 48, at 26).

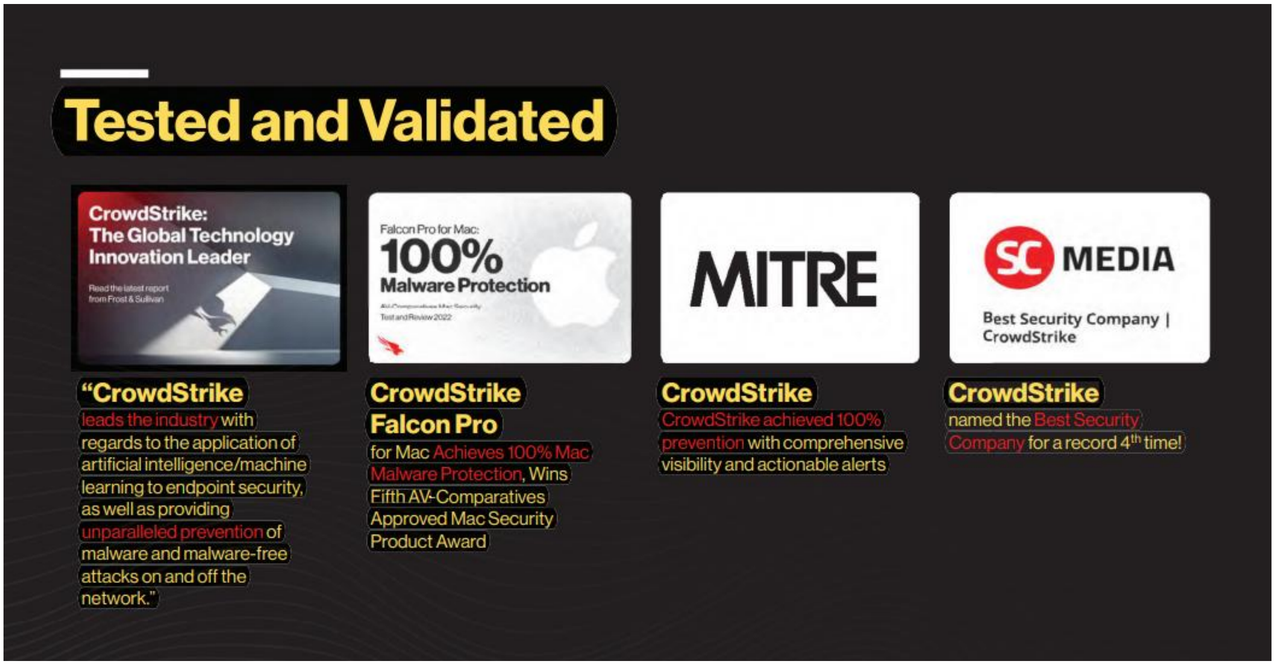
The Court agrees with Plaintiffs that it would be improper to determine at this early stage of the litigation whether Rapid Response updates were understood by investors to be software or code. Unlike the above-discussed representations made by Defendants where context clarified allegedly misleading or false statements, Defendants do not support this argument with any materials from before the July 2024 outage that Court may consider at this stage of the litigation. As Plaintiffs argue, Defendants' post-hac characterizations of Rapid Response Content—e.g., Adam Meyers's testimony before Congress—do not aid the Court in determining what a reasonable investor would have understood *prior* to the July 2024 outage. (Pls.' Resp., Dkt. 48, at 26). Moreover, despite taking judicial notice of Meyer's testimony, the Court cannot accept at the motion-to-dismiss stage his assertion that Rapid Response Content updates are not software or code. *See Linenweber*, 696 F.

Supp. 3d at 674. The Court will therefore accept Plaintiffs' allegations that the outage was caused by a software update or updated code.

The first statement related to software that Plaintiffs challenge as misleading or false is Defendant Kurtz's statement, "Testing and validation is really important. We test more than anyone else, more than all of our next-gen competitors, more than other players that are out there." (Compl., Dkt. 41, at 52, 68). Plaintiffs allege that this statement was false or misleading because (1) CrowdStrike did not test its software updates in a pre-production environment; (2) CrowdStrike lacked a quality assurance team and failed to have industry-standard test plans for its software updates; and (3) CrowdStrike prioritized speed over quality control. (*Id.* at 68).

Defendants argue in their motion to dismiss that "[a]gain, [Plaintiffs] strip[] this statement of its context and mischaracterizes it." (Mot. to Dismiss, Dkt. 47, at 25). They stress that Kurtz made this statement while giving a presentation about third-party testing and validation of the Falcon's efficacy at preventing breaches—not for preventing crashes or other performance issues. (*Id.*). Plaintiffs respond that "[a]t most, Defendants' self-serving characterization of [this] statement raises a factual dispute" to be resolved by a jury. (Pls.' Resp., Dkt. 48, at 29).

As noted in Section III(A), *supra*, the Court has considered the transcript of the investor briefing where Kurtz made this statement, as the briefing was referenced by Plaintiffs and is central to their claim. The transcript of this investor briefing shows that the sentences spoken by Kurtz directly after the one quoted by Plaintiffs are: "And when you look at the results, 100% protection . . . [the] test couldn't even run until we turned off some of the identity elements, named the best security company for a record fourth time, you can see the leadership. . . . Our technology is better than the other companies that are out there. . . . and the testing results prove it." Moreover, when Kurtz made this statement, this slide was being presented:



Tested and Validated

CrowdStrike:
The Global Technology
Innovation Leader

Read the latest report
from Frost & Sullivan

"CrowdStrike leads the industry with regards to the application of artificial intelligence/machine learning to endpoint security, as well as providing unparalleled prevention of malware and malware-free attacks on and off the network."

Falcon Pro for Mac:
100%
Malware Protection
AV-Comparatives Mac Security
Test and Review 2022

CrowdStrike Falcon Pro for Mac Achieves 100% Mac Malware Protection, Wins Fifth AV-Comparatives Approved Mac Security Product Award

MITRE

CrowdStrike

CrowdStrike achieved 100% prevention with comprehensive visibility and actionable alerts

SC MEDIA

Best Security Company |
CrowdStrike

CrowdStrike

named the Best Security Company for a record 4th time!

(CrowdStrike 2022 Investor Briefing Slides, Dkt. 47-26, at 11). Viewing Defendant Kurtz's statement in context, it is obvious that he was speaking about CrowdStrike's testing of the software's purpose—to prevent security breaches. No reasonable investor would understand Kurtz to have been talking about CrowdStrike's testing of its software to find bugs and prevent crashes. He made no reference whatsoever to CrowdStrike's software development process. The Court therefore agrees with Defendants that, again, *Plaintiffs* have made a misleading statement here—not Defendants.

Second, Plaintiffs challenge Defendant Sentonas's statement during an April 2023 investor briefing that CrowdStrike's "agent cloud architecture . . . . doesn't require a massive tuning burden and doesn't blue screen endpoints with failed updates." (Compl., Dkt. 41, at 69). Plaintiffs allege that it was false or misleading for Sentonas to state that Falcon "doesn't blue screen endpoints with failed updates" while "omitting" that CrowdStrike did not test its software updates according to industry practices and prioritized speed over quality control, "which directly exposed its user-endpoints to bluescreening." (*Id.*).

Defendants argue in their Motion to Dismiss that Sentonas's statement "does not purport to guarantee that CrowdStrike would *never* cause a blue screen outage." (Mot. to Dismiss, Dkt. 47, at 23). They also point out that Plaintiffs fail to plead any particularized facts showing that Sentonas's statement was false when made, as Plaintiffs do not allege that a Falcon software update had caused any endpoints to blue screen when Sentonas made that assertion in April 2023. (*Id.*). Plaintiffs respond that Sentonas's statement was "not limited to the past," meaning Sentonas was "required, but failed, to disclose the 'full truth,' including CrowdStrike's failure to test its updates and lack of quality assurance," which heightened the risk that a Falcon update could cause a computer to crash. (Pls.' Resp., Dkt. 48, at 21). Defendants reply that they repeatedly disclosed to investors the risk of an outage from software updates. (Defs.' Reply, Dkt. 55, at 9).

The Court agrees with Defendant that this statement by Defendant Sentonas is not actionable. First of all, Sentonas's statement that "our agent cloud architecture . . . . doesn't blue screen end points with failed updates, which happens a lot across the industry," (Dkt. 47-22, at 7), is arguably immaterial puffery. It is a "generalized, positive statement[] about the company's competitive strengths" that is "not specific enough" to support a securities fraud action. *See Southland Sec. Corp. v. INSpire Ins. Sols., Inc.*, 365 F.3d 353, 372 (5th Cir. 2004) (quoting *Lain v. Evans*, 123 F. Supp. 2d 344, 348 (N.D. Tex. 2000)).

Plus, even if this statement were not immaterial puffery, there is an additional reason this statement is not actionable. The Court "has reviewed the relevant public filings and determines that they adequately warned investors of exactly the risks Plaintiffs contend were not disclosed." *See In re Capstead Mortg. Corp. Sec. Litig.*, 258 F. Supp. 2d 533, 555 (N.D. Tex. 2003). CrowdStrike's 2023 and 2024 Annual Reports, (Dkts. 47-7, 47-24) each warn:

> Our customers depend on the continuous availability of our Falcon platform. . . . We have experienced, and expect that in the future we may experience interruptions, delays and outages in service and availability from time to time due to a variety of factors, including . . . human or software errors . . . . The following factors, many of

> which are beyond our control, can affect the delivery, availability, and performance of our Falcon platform:
> . . .
> - errors, defects or performance problems in our software . . . .
> - improper deployment or configuration of our solutions . . . .
>
> . . .
> The adverse effects of any service interruptions on our reputation, results of operations, and financial condition may be disproportionately heightened due to the nature of our business and the fact that our customers have a low tolerance for interruptions of any duration. . . . While we do not consider them to have been material, we have experienced, and may in the future experience, service interruptions and other performance problems due to a variety of factors."

(FY 2023 Annual Report, Dkt. 47-24, at 28–30; FY 2024 Annual Report, Dkt. 47-7, at 30–31). The 2023 and 2024 Annual Reports also state: "**If our solutions . . . have or are perceived to have defects, errors, or vulnerabilities, our brand and reputation would be harmed, which would adversely affect our business and results of operations**. . . . Because our cloud native security platform is complex, it may contain defects or errors that are not detected until after deployment." (FY 2023 Annual Report, Dkt. 47-24, at 27; FY 2024 Annual Report, Dkt. 47-7, at 29) (emphasis in original). In light of these risk warnings in CrowdStrike's Annual Reports, no reasonable investor would have relied on Sentonas's vague statement of corporate cheerleading that CrowdStrike's software does not blue screen computers. *See In re Azurix Corp. Sec. Litig.*, 198 F. Supp. 2d 862, 884 (S.D. Tex. 2002) ("[B]ecause plaintiffs could not have relied on any of the statements in the prospectus, in light of [the defendant's] risk warnings and because the statements were merely expressions of corporate optimism, the court concludes that these claims are not actionable.").

Third, Plaintiffs allege that CrowdStrike made a false or misleading statement when it stated in a November 2021 blog post that "[f]or system stability, we always do canary deployments of new services before rolling out changes to the entire fleet." (Compl., Dkt. 41, at 36). They claim this statement is false or misleading because the update that caused the July 2024 outage was released to every customer simultaneously. (*Id.* at 36–37). Defendants contend in their Motion to Dismiss that

Plaintiffs failed to allege the statement in the blog post was false because they did not allege that the July 2024 content update was a "new service." (Mot. to Dismiss, Dkt. 47, at 23). Defendants also argue that no reasonable investor would interpret "new services" to include Rapid Response Content updates, considering: (1) they are "regular, automatic" updates; (2) this sentence was taken from a blog post about "JSON Marshaling," which "describes the process of converting data structures" into a certain format; and (3) CrowdStrike has "long disclosed" that Rapid Response Content updates are automatically transmitted to all customers. (*Id.* at 23, 29). Plaintiffs respond that CrowdStrike's disclosures that their software engages in "real-time" protection does not "trump[] their representation that 'we always do canary deployments,'" and does not inform investors that CrowdStrike was "shirk[ing] the industry-standard practice of phased rollouts." (Pls.' Resp., Dkt. 48, at 31).

A reasonable investor viewing CrowdStrike's 2023 and 2024 Annual Reports on the one hand, (Dkts. 47-7, 47-24), and viewing an obscure CrowdStrike blog post on the other hand, (Dkt. 47-23), would not be misled into believing that CrowdStrike's Rapid Response Content updates are sent out to customers in phased rollouts. CrowdStrike's public disclosures emphasize the exact opposite—that the Falcon platform "automates detection and prevention capabilities **in real time across [its] entire global customer base**." (2023 Annual Report, Dkt. 47-24, at 6; 2024 Annual Report, Dkt. 47-7, at 6) (emphasis added). Similarly, the 2023 Annual Report celebrates that one of the "[k]ey benefits of . . . the CrowdStrike Falcon platform" is its ability to "**automatically** deliver[] protection **to every customer**." (2023 Annual Report, Dkt. 47-24, at 9) (emphasis added). The idea that a reasonable investor would (1) read a highly technical November 2021 blog post about "JSON Marshaling, "[17] (2) believe a sentence in that blog post about canary rollouts of new services applies

[17] According to Defendants, JSON marshaling "describes the process of converting data structures into a JavaScript Object Notation . . . format." (Mot. to Dismiss, Dkt. 47, at 23).

to Falcon's Rapid Response Content updates, and (3) then rely on that belief instead of clear disclosures to the contrary in CrowdStrike's official SEC filings, is implausible as a matter of law.[18] The Court therefore finds that Plaintiffs have not sufficiently pleaded that the sentence about canary rollouts within the JSON Marshaling blog post was a material misstatement.

Fourth and fifth, Plaintiffs challenge statements in CrowdStrike's 2023 and 2024 Annual Reports that "[CrowdStrike's] technical staff monitors and tests our software on a regular basis," and that "[CrowdStrike] also maintain[s] a regular release process to update and enhance our existing solutions." (2024 Annual Report, Dkt. 47-7, at 18; 2023 Annual Report, Dkt. 47-24, at 17). They plead that it was false or misleading for CrowdStrike to assure investors that it tests its software on a regular basis and has a regular release process without disclosing that it released certain software updates without any process, without testing in a pre-production environment, and without a quality assurance team. (Compl., Dkt. 41, at 74).

Defendants maintain in their Motion to Dismiss that these are generalized statements that CrowdStrike regularly tests and updates Falcon's software, rather than being representations about specific features of the testing and updating processes used for Rapid Response Content updates, and that these statements make no guarantee of their processes' effectiveness. (Mot. to Dismiss, Dkt. 47, at 24). Defendants also argue that these statements are nonactionable because they are immaterial puffery. (*Id.* at 24 n.4). Plaintiffs emphasize in their response that these statements were false because CrowdStrike "had no 'process' at all, beyond simultaneously thrusting [updates] upon

[18] The Court also takes issues with how Plaintiffs framed this allegation. Plaintiffs alleged: "Despite telling investors that it abided by this industry standard—with CrowdStrike stating that 'we *always* do canary deployments of new services before rolling out changes to the entire fleet'—the Company did not do so." (Compl., Dkt. 41, at 36) (emphasis added by Plaintiffs). It strains credulity for Plaintiffs to plead that an obscure, highly technical blog post written by an engineer is equivalent to CrowdStrike "telling investors"—who were surely not the intended or expected audience of the blog post—anything at all.

all customers the moment they were complete." (Pls.' Resp., Dkt. 48, at 29). Plaintiffs do not respond to Defendants' argument that these statements were nonactionable puffery.

First, the Court holds that Plaintiffs have failed to plausibly allege that CrowdStrike's statement that it "maintain[s] a regular release process to update and enhance our existing solutions" was false or misleading. Plaintiffs themselves acknowledge that Falcon received "automatic 'updates.'" (Compl., Dkt. 41, at 13). They therefore did not allege that Falcon did not release regular updates. Plus, even taking as true Plaintiffs' assertion that CrowdStrike did not properly test certain updates, CrowdStrike's claim that it regularly releases updates is not a representation to investors about the *efficacy* of those updates. *See Linenweber*, 693 F. Supp. 3d at 678–79. (explaining that "[r]egular [maintenance] checks are consistent or structured checks, not immediate or exhaustive ones" and noting that checks may be done both regularly and "imperfect[ly]"). Moreover, the Court finds CrowdStrike's statement that it uses updates to "enhance [its] existing solutions" to be a "generalized, positive statement[] about the company's competitive strengths," rather than a fact specific enough to be actionable. *See Rosenzweig v. Azurix Corp.*, 332 F.3d 854, 869 (5th Cir. 2003) (citing *Raab v. Gen. Physics Corp.*, 4 F.3d 286, 290 (4th Cir. 1993)). *See also, e.g.*, *Nathenson v. Zonagen Inc.*, 267 F.3d 400, 419 (5th Cir. 2001) (holding that a statement by defendants that a medication was an "improved formulation" was "nothing more than inactionable 'puffing'"); *Rosenzweig*, 332 F.3d at 870 (holding that a press release's assertion that a company was "making steady progress" is "precisely the sort of generalized positive characterization that is not actionable under the securities laws"); *Linenweber*, 693 F. Supp. 3d at 675–76 (holding that a press release stating that "we continually work to create and foster a Culture of Safety" was "aspirational puffery . . . and not actionable fraud").

Second, the Court holds that Plaintiffs have failed to adequately plead that the statement, "Our technical staff monitors and tests our software on a regular basis," was false or misleading.

CrowdStrike disclosed—in fact, widely promoted, according to Plaintiffs—that its Rapid Response Content updates were sent to the Falcon sensor automatically and in real time. As Plaintiffs allege in their Complaint, Rapid Response Content updates being automatic and responsive to real-time data was "a centerpiece of [Falcon's] value proposition to both customers and investors" and was "central to CrowdStrike's investment thesis." (Compl., Dkt. 41, at 13). The Court is highly skeptical that reasonable investors, who were allegedly motivated to invest in CrowdStrike at least in part *because* of its novel Rapid Response technology, would both (1) appreciate that Rapid Response Content updates were automatic and based on real-time data, and (2) nonetheless believe that Rapid Response Content updates went through normal testing and roll-out procedures. To the contrary, it is significantly more plausible that a reasonable investor would understand that Rapid Response Content updates are not tested or rolled out like normal software or code updates.[19]

4. Statements About Regulatory Compliance

Finally, two of the alleged misstatements are related to CrowdStrike's regulatory compliance. CrowdStrike represented in online materials that it meets the compliance requirements for U.S. FedRAMP and for Department of Defense Impact Level 4. (Compl., Dkt. 41, at 29; CrowdStrike FedRAMP FAQ, Dkt. 47-27, at 2; CrowdStrike White Paper on Solutions for Federal Agencies, Dkt. 47-28, at 8). According to Plaintiffs, these statements were false or misleading because FedRAMP and DoD requirements mandate that software companies:

> (i) test new updates in a preproduction environment that replicates the production environment such software will run on when released to customers, (ii) utilize a phased rollout process to ensure that errors are identified in a small number of

[19] Additionally, the Court again notes that CrowdStrike warned investors that its "cloud native security platform is complex [and] may contain defects or errors that are not detected until after deployment." (FY 2023 Annual Report, Dkt. 47-24, at 27; FY 2024 Annual Report, Dkt. 47-7, at 29). There was no guarantee of Falcon being implemented perfectly, and CrowdStrike disclosed that, "due to the nature of [its] business and the fact that our customers have a low tolerance for interruptions of any duration," the "adverse effects of any service interruptions on [CrowdStrike's] reputation, results of operations, and financial condition may be disproportionately heightened." (FY 2023 Annual Report, Dkt. 47-24, at 28–30; FY 2024 Annual Report, Dkt. 47-7, at 30–31).

> production environments before updates are released to the vast majority of customers, and (iii) maintain quality assurance staff distinct from software developers to conduct such testing and in accordance with standardized test plans.

(Compl., Dkt. 41, at 30). They also allege that companies seeking FedRAMP or DoD authorization must explicitly certify that they meet the above requirements and that "Defendant Kurtz or someone else in the C-Suite, including Defendant Sentonas, had to sign" such certifications. (*Id.*). Plaintiffs claim that, in fact, CrowdStrike was not meeting these requirements, "including their requirements to test software updates in a separate test environment that replicates the operational system prior to the release of the software update and to maintain a dedicated quality assurance team to conduct quality assurance and testing of software updates." (*Id.* at 76–77).

In response to these allegations, Defendants have two main arguments in their Motion to Dismiss: (1) The Court may take judicial notice of the fact that, according to the federal government's website, CrowdStrike *is* authorized by both FedRAMP and DoD, and (2) Plaintiffs misrepresent the NIST standards that underlie FedRAMP and DoD requirements. (Mot. to Dismiss, Dkt. 47, at 12). Regarding their second argument, Defendants claim that three of the four NIST standards Plaintiffs allege CrowdStrike violated are "*not required* for Moderate FedRAMP authorization or DoD Impact Level 4 authorization, which are the authorizations that [Plaintiffs] allege[] CrowdStrike held on July 19, 2024." (Mot. to Dismiss, Dkt. 47, at 28). As to the fourth NIST standard, Defendants assert that Plaintiffs' reading of the requirement—that it requires a quality assurance team for testing software—is not supported by the text of the requirement. (*Id.*). The requirement, AC-5, is called "Separation of Duties." (NIST Standards, Dkt. 47-29, at 9). It states in the supplemental guidance section: "Separation of duties includes, for example . . . (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security)." (*Id.*) Defendants argue AC-5 "merely requires that certain duties be performed by separate individuals or teams, and *as an example*, mentions separating 'information system support functions, *such as* 'quality assurance and testing.'" (Mot. to Dismiss, Dkt. 47, at 28) (emphasis in original).

First, regarding CrowdStrike's statement that it "meets the . . . compliance requirements" of FedRAMP and DoD Impact Level 4, the Court disagrees that CrowdStrike being designated as authorized under these programs nullifies Plaintiffs' allegation that CrowdStrike was failing to meet the requirements of those programs. Plaintiffs did not allege that CrowdStrike is not authorized by those programs; rather, they allege that CrowdStrike falsely certified that they are meeting those programs' requirements in order to become certified. The Court therefore rejects Defendants' argument that CrowdStrike being designated as authorized makes Plaintiffs' allegation fail.

Second, regarding Defendants' argument about the four NIST standards Defendants allegedly violated, the Court ultimately again disagrees that Plaintiffs' allegations are implausible. The Court takes judicial notice of NIST Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, (Dkt. 47-29),[20] as a government publication.[21] This government publication patently shows that NIST SP 800-53 standards CM-2(6), CM-4(1), and SA-15 do not apply to organizations authorized at the Moderate level.[22] Plaintiffs do not dispute that CrowdStrike was authorized at DoD Impact Level 4 and had FedRAMP Moderate authorization during the class period.[23] Yet Plaintiffs argue that, regardless of CrowdStrike not being

[20] In addition to being available on the docket, (Dkt. 47-29), this publication is available at http://dx.doi.org/10.6028/NIST.SP.800-53r4.

[21] *See, e.g.*, *Kitty Hawk Aircargo, Inc. v. Chao*, 418 F.3d 453, 457 (5th Cir. 2005) (taking judicial notice of information on a government website); *Coleman v. Dretke*, 409 F.3d 665, 667 (5th Cir. 2005) (per curiam) (taking judicial notice of a Texas agency's website).

[22] These requirements relate to standards for testing software prior to implementation and to documentation of the development process. (NIST Standards, Dkt. 47-29, at 10–17).

[23] Plaintiffs do argue for the first time in their Response to the Motion to Dismiss that CrowdStrike told investors it was FedRAMP High-Impact Level Ready. (Pls.' Resp., Dkt. 48, at 33). Plaintiffs did not make this allegation in their Complaint, so it is not before the Court. *See Roebuck v. Dothan Sec., Inc.*, 515 F. App'x 275, 280 (5th Cir. 2013) (per curiam) (holding that district courts ruling on a motion to dismiss are "limited to the allegations set forth the complaint" and cannot rely upon facts only set forth in the plaintiff's briefing in opposition to a motion to dismiss); *Dorsey v. Portfolio Equities, Inc.*, 540 F.3d 333, 338 (5th Cir. 2008) ("Because

required to meet the requirements of CM-6(2), CM-4(1), and SA-15, Defendants did not make clear that CrowdStrike's software was only meeting the Moderate-level requirements, rather than all of the requirements listed. (Pls.' Resp., Dkt. 48, at 32–33). For example, CrowdStrike represented that it was "meeting the stringent requirements" of FedRAMP. (Compl., Dkt. 41, at 29). CrowdStrike also stated in a white paper for federal agencies that it meets "U.S. FedRAMP program requirements" without specifying the *level* of requirements it meets. (CrowdStrike White Paper on Solutions for Federal Agencies, Dkt. 47-28, at 8). Plaintiffs contend that whether a reasonable investor would understand that statement to be limited to Moderate-level requirements is a fact issue that cannot be properly decided at this stage. (Pls.' Resp., Dkt. 38, at 32).

Though it is a close call, the Court finds it plausible that an investor would interpret meeting "FedRAMP program requirements" and "the stringent requirements" of FedRAMP as meeting the high-level requirements of that program. This conclusion is informed by "surrounding text," which touts, "Meeting these stringent requirements reinforces CrowdStrike's commitment and ability to serve customers of all types . . . . [T]he Falcon platform has been audited and validated **against some of the strictest security requirements in the world**." (CrowdStrike Webpage on FedRAMP, Dkt. 47-27, at 2). *See Omnicare*, 575 U.S. at 190 ("[A]n investor reads each statement . . . in light of all its surrounding text . . . ."). And, significantly, meeting the high-level requirements for FedRAMP would surely be material to an investor. For instance, CrowdStrike allegedly told investors that compliance with DoD's requirements "positions us well to extend our reach into the massive defense IT and cybersecurity markets." (Compl., Dkt. 41, at 29).

Additionally, though Defendants' argument that AC-5 does not *require* a quality assurance team separate from its programming team is well-taken, the Court is unwilling to interpret AC-5 as a

the court reviews only the well-pleaded facts in the complaint, it may not consider new factual allegations made outside the complaint . . . .").

matter of law at this stage. Defendants fault Plaintiffs for not citing any authority interpreting AC-5 in support of their argument—but neither do Defendants. (See Mot. to Dismiss, Dkt. 47, at 28; Defs.' Reply, Dkt. 55, at 16). It appears that no court has interpreted AC-5 regarding whether it mandates a quality assurance team, and the Court will not make such a determination at the motion-to-dismiss stage where competing interpretations are plausible.

Based on the above reasoning and on Plaintiffs' allegations that CrowdStrike did not have a separate quality assurance team as mandated by federal requirements that CrowdStrike certified it was meeting, the Court finds that Plaintiffs have plausibly alleged two statements to be false or misleading: (1) "CrowdStrike meets the following compliance requirements: U.S. FedRAMP program requirements; Department of Defense Impact Level 4 (IL-4)," and (2) "Meeting these stringent requirements [related to FedRAMP and DoD cloud authorizations] reinforces CrowdStrike's commitment and ability to serve customers of all types by safeguarding their enterprises with the most effective endpoint protection platform and ultimately stopping breaches." (CrowdStrike White Paper on Solutions for Federal Agencies, Dkt. 47-28, at 8; CrowdStrike FedRAMP FAQ, Dkt. 47-27, at 2).

C. Scienter

In Section III(B), *supra*, the Court found that, out of the fifteen statements put forth by Plaintiffs, Plaintiffs have plausibly alleged two false or misleading statements. These two statements are unattributed. (CrowdStrike White Paper on Solutions for Federal Agencies, Dkt. 47-28, at 8; CrowdStrike FedRAMP FAQ, Dkt. 47-27, at 2). Nonetheless, because motions to dismiss under 12(b)(6) are "viewed with disfavor" and should be "rarely granted," *see Turner*, 663 F.3d at 775, the Court will review Plaintiffs' allegations of scienter for all three Defendants.

The PSLRA specifically requires that a complaint in a securities case "state with particularity facts giving rise to a strong inference that the defendant acted with the required state of mind." 15

U.S.C. § 78u-4(b)(2)(A). "In 10b-5 actions, 'scienter' ranges from intentional deception to severe recklessness, the latter being defined as 'an extreme departure from the standards of ordinary care, [presenting] 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.'" *Masel v. Villareal*, 924 F.3d 734, 747 (5th Cir. 2019) (quoting *Rosenzweig*, 332 F.3d at 866). To evaluate scienter at the motion-to-dismiss stage, a court must (1) take the well-pleaded allegations as true; (2) evaluate the facts collectively, including facts contained in "documents incorporated in the complaint by reference and matters subject to judicial notice," "determine whether a strong inference of scienter has been pled"; and (3) "take into account plausible inferences opposing as well as supporting a strong inference of scienter."[24] *Alaska Elec. Pension Fund*, 915 F.3d at 982 (quoting *Ind. Elec. Workers' Pension Tr. Fund IBEW v. Shaw Grp., Inc.*, 537 F.3d 527, 533 (5th Cir. 2008)).

Scienter must be specifically pleaded for each defendant. *Southland Sec. Corp.*, 365 F.3d at 365 ("[T]he PSLRA requires the plaintiffs to distinguish among those they sue and enlighten *each defendant* as to his or her particular part in the alleged fraud.") (emphasis in original). Pleadings of scienter "may not rest on the inference that defendants must have been aware of a misstatement based on their positions with the company." *Abrams v. Baker Hughes, Inc.*, 292 F.3d 424, 432 (5th Cir. 2002) (citing *In re Advanta Corp. Sec. Litig.*, 180 F.3d 525, 539 (3d Cir. 1999)). Finally, scienter normally may be attributed to a defendant corporation "when the requisite scienter is found for the individual officer of that corporation who made the false or misleading statement," though it may be "possible to draw a strong inference of corporate scienter without being able to name the individual" who made the statement where the statement was "so dramatic 'it would have been approved by corporate officials sufficiently knowledgeable about the company to know that the

[24] To create a strong inference of scienter, the inference must be "at least as compelling as any opposing inference one could draw from the facts alleged." *Tellabs*, 551 U.S. at 324.

announcement was false." *In re Dell Inc., Sec. Litig.*, 591 F. Supp. 2d 877, 899 (W.D. Tex. 2008) (first citing *Southland Sec. Corp.*, 365 F.3d at 366; and then quoting *Makor Issues & Rights, Ltd. v. Tellabs, Inc.*, 513 F.3d 702, 710 (7th Cir. 2008)).

Defendants make four primary arguments in support of their claim that Plaintiffs failed to effectively plead scienter. First, Defendants contend that Plaintiffs have failed to allege a theory of motive, which raises Plaintiffs' burden to plead strong circumstantial evidence of scienter. (Mot. to Dismiss, Dkt. 47, at 32–33). Second, Defendants assert that Plaintiffs' alleged allegations in support of scienter—including allegations from former employers, evidence of prior faulty updates, post-outage statements from Defendants, and other "miscellaneous" allegations—are not strong enough to meet their burden. (*Id.* at 33–39). Third, Defendants argue that Plaintiffs, as to the alleged misstatements posted on CrowdStrike's website, failed to plead particularized facts showing that Defendants "Kurtz and Sentonas made, approved, or were even aware of these statements." (*Id.* at 39). Lastly, Defendants assert that the more plausible inference is that Defendants thought their testing of Rapid Response Content updates was sufficient. (*Id.* at 40). For the reasons set for below, based on a holistic view of the allegations, *see Owens*, 789 F.3d at 536–37, the Court finds Plaintiffs have failed to raise a strong inference of scienter.

1. Motive

Though "absence of a motive allegation is not fatal," *Tellabs*, 551 U.S. at 325, motive "is a critical . . . aspect of a successful claim for securities fraud." *Mun. Employees' Ret. Sys. Of Mich. v. Pier 1 Imports, Inc.*, 935 F.3d 424, 431 (5th Cir. 2019) (citing *Abrams*, 292 F.3d at 434). To allege motive, plaintiffs must plead "concrete benefits that could be realized by one or more of the false statements and wrongful nondisclosures alleged." *Id.* at 430–31 (quoting *Shaw Grp.*, 537 F.3d at 543). When a plaintiff fails to plausibly plead motive, "the strength of the circumstantial evidence of scienter must be correspondingly greater." *Id.* at 431 (quoting *Neiman v. Bulmahn*, 854 F.3d 741, 748 (5th Cir. 2017)).

Though Plaintiffs phrase their motive allegation in a variety of ways, they provide the Court with essentially one motive allegation: "Defendants Kurtz and Sentonas personally established and maintained [a] culture at CrowdStrike" of prioritizing speed "to maximize short-term profits [and] to artificially inflate CrowdStrike's stock price and their own personal net worths." (Compl., Dkt. 41, at 8, 32–33, 39, 65). This allegation does not lead to a proper inference of scienter. In the Fifth Circuit, allegations that "defendants were motivated to commit fraud by the need to raise capital, the desire for enhanced incentive compensation[,] and the desire to sell stock at inflated prices" are—without more—"insufficient to support an inference of scienter."[25] *Abrams*, 292 F.3d at 434. If such allegations were sufficient, "the executives of virtually every corporation in the United States would be subject to fraud allegations." *Tuchman*, 14 F.3d at 1068 (citation omitted). The Court also "note[s] . . . that there is no allegation that [D]efendants sold their [CrowdStrike] shares, calling into question the alleged motive to artificially inflate the stock price." *See Rosenzweig*, 332 F.3d at 867. Nor are there other allegations in the Complaint explaining how Defendants profited from their alleged misstatements, other than the conclusory allegation that Defendants acted to inflate their own net worths.

Plaintiffs have therefore failed to plead a plausible motive for Defendants to commit securities fraud. Thus, for Plaintiffs to survive this motion to dismiss, the Court will require Plaintiffs' other allegations regarding scienter to overcome an even higher bar. *See Tellabs*, 551 U.S. at

[25] Moreover, unlike in *Goldstein v. MCI WorldCom*, 340 F.3d 238 (5th Cir. 2003), Plaintiffs have not alleged the existence of a unique circumstance giving Defendants an even greater need to raise capital than normal. *See Neiman*, 854 F.3d at 748 (quoting *Shaw Grp.*, 537 F.3d at 544) (explaining *Goldstein* as an "outlier" to the proposition that "the desire to raise capital in the normal course of business does not support a strong inference of scienter," because the company in *Goldstein* needed "to complete a 'crucial' $129 billion merger," which "gave the company a motive to inflate its financial results").

325; *Neiman*, 854 F.3d at 748; *Tuchman*, 14 F.3d at 1068 (citing *Beck v. Manufacturers Hanover Tr. Co.*, 820 F.2d 46, 50 (2d Cir. 1987)) ("Where a defendant's motive is not apparent, a plaintiff may adequately plead scienter by identifying circumstances that indicate conscious behavior on the part of the defendant, though the strength of the circumstantial allegations must be correspondingly greater.")

2. Statements Supporting Defendants' Knowledge of Testing Deficiencies

Plaintiffs allege that Defendants knew, or were severely reckless in not knowing, that their statements about CrowdStrike's testing processes were false or were misleading by omission. (Compl., Dkt. 41, at 55). In support of this allegation, Plaintiffs plead that: (1) Defendants were warned by former employees of testing deficiencies; (2) Defendants were aware of previous faulty updates; (3) Defendants made post-outage statements admitting fault; and (4) other miscellaneous allegations point towards fraudulent intent. The Court will consider each of these categories of allegations in turn and then holistically.[26]

a. Former Employee Warnings

First, Plaintiffs allege that former employees "sounded the alarm . . . about the deficient testing and quality control in place within [CrowdStrike] during the Class Period." (Compl., Dkt. 41, at 61). FE-5, a former "Onboarding Technical Account Manager and Provisioning Engineer," claims that CrowdStrike "lacked a quality assurance team" and "agreed that Defendants Kurtz and Sentonas would have known that fact." (*Id.* at 38, 62). He further alleges that, around March 2024, he "sent a video message directly to Defendants Kurtz and Sentonas, warning them about understaffing issues he had observed, including for key support and engineering teams, which left

[26] "A district court may best make sense of scienter allegations by first looking to the contribution of each individual allegation to a strong inference of scienter, especially in a complicated case such as this one. Of course, the court must follow this initial step with a holistic look at all the scienter allegations." *Owens*, 789 F.3d at 537.

critical issues unaddressed." (*Id.* at 40, 62). According to FE-5, he was told that Defendants Kurtz and Sentonas watched his video. (*Id.* at 40).

Plaintiffs also point to an article published by an investigative journalist as strengthening an inference of scienter. (*Id.*; Semafor Article, Dkt. 47-6). Former CrowdStrike software engineers claim in the article that they had raised concerns about lack of quality assurance processes and had complained about "rushed deadlines, excessive workloads, and increasing technical problems to high-ups for more than a year before" the July 2024 outage. (Compl., Dkt. 41, at 40). Plaintiffs argue that these allegations from former employees strengthen the scienter inference. (*Id.* at 62–63).

The Court agrees with Defendants that these allegations do not lead to a strong inference of scienter. FE-5 allegedly warning Defendants Kurtz and Sentonas about "understaffing" causing "critical issues [to be] unaddressed" is not specific enough for the Court to plausibly infer that Defendants Kurtz and Sentonas knew or were severely reckless in not knowing that statements they made about quality assurance or testing of Rapid Response Content updates were false or misleading. *See Owens*, 789 F.3d at 544 (reasoning that an email from a confidential source did not lead to an inference on scienter because it did not mention the specific issue the defendants allegedly knew about); *Mun. Employees' Ret. Sys. Of Mich.*, 935 F.3d at 433 (holding that an alleged warning of "amorphous 'inventory problems'" was too vague to show a defendant knew of a specific inventory problem).

The allegations based on the investigative journalist's article are also weak. Many of the former employees cited have little information included about them to support their credibility, such as what time period they worked at CrowdStrike.[27] *See Cent. Laborers' Pension Fund v. Integrated Elec.*

[27] For instance, Plaintiffs quote from the article: "Almost two dozen former software engineers, managers and other staff described a workplace where executives prioritized speed over quality, workers weren't always sufficiently trained, and mistakes around coding and other tasks were rising." (Compl., Dkt. 41, at 40). Such a vague descriptor of these confidential sources comes nowhere close to meeting the Fifth Circuit's requirement that confidential sources be described "with sufficient particularly to support the probability that

Services Inc., 497 F.3d 546, 552 (5th Cir. 2007) (holding that confidential source allegations were not credible where the allegations lacked "particular job descriptions, individual responsibilities, and specific employment dates"). Moreover, none of the allegations Plaintiffs rely upon from the journalist's article support that Defendants Kurtz or Sentonas in particular knew of certain information that would make their future statements false or misleading; instead, the allegations refer vaguely to "company leaders" or "higher-ups."[28] (Compl., Dkt. 41, at 8, 40–41, 62). Such ambiguous allegations, especially in light of the Fifth Circuit's rule that "courts must discount allegations from confidential sources," do not support a strong inference of scienter. *See Mun. Employees' Ret. Sys. Of Mich.*, 935 F.3d at 433 (quoting *Shaw Grp.*, 537 F.3d at 535).

b. Prior Faulty Updates

Next, Plaintiffs allege that CrowdStrike had previously released faulty Falcon updates in April and May 2024. (Compl., Dkt. 41, at 63). According to Plaintiffs, that Defendants "previously released faulty software updates" in the past but "continued to make misrepresentations about CrowdStrike's quality assurance processes for its updates" strengthens the scienter interference. (*Id.* at 64). Defendants argue, *inter alia*, that Plaintiffs fail to make any allegations supporting that Defendants Kurtz or Sentonas knew of these faulty software updates. (Mot. to Dismiss, Dkt. 47, at 36). Plaintiffs do not rebut this argument in their Response, though they do allege in their Complaint that Defendant Sentonas, as the President and Chief Technology Officer of CrowdStrike, was "the executive specifically responsible for the Falcon platform," "oversaw the development of its

a person in the position occupied by the source . . . would possess the information pleaded . . . ." *See Shaw Grp.*, 537 F.3d at 535 (quoting *ABC Arbitage Plaintiffs Grp.*, 291 F.3d at 353).

[28] For example, Plaintiffs quote from the article that a "former senior manager said they sat in multiple meetings where staff warned company leaders that CrowdStrike would 'fail' its customers by releasing products that couldn't be supported." (Compl., Dkt. 41, at 41). There is no allegation that these "company leaders" included Defendants Kurtz or Sentonas.

software, including its testing of its software updates," and had a "role and responsibilities at CrowdStrike [that] further strengthen[] the scienter inference." (Compl., Dkt. 41, at 66).

What Plaintiffs are asking the Court to do—infer knowledge of false or misleading statements based solely on Defendants' positions at CrowdStrike—is impermissible under explicit Fifth Circuit precedent. *See Shaw Grp.*, 537 F.3d at 540 (quoting *Abrams*, 292 F.3d at 432) (noting that the Fifth Circuit has rejected the "'defendants must have known' allegation" based on a defendant's position in the company "as too vague to support a strong inference of scienter"). Thus, the April and May 2024 alleged faulty updates do not allow the Court to infer a strong inference of scienter, as there is no non-conclusory allegation that Defendants Kurtz or Sentonas knew of these faulty updates or were severely reckless in not knowing they occurred.[29]

c. Post-Outage Statements

Third, Plaintiffs assert that CrowdStrike's post-incident reports were "understood . . . as admissions that [CrowdStrike's] testing and quality assurance practices were deficient and ***not*** as previously represented." (Compl., Dkt. 41, at 51) (emphasis in original). They also point to statements made by CrowdStrike executives after the July 2024 incident as evidence of scienter. Defendant Sentonas, referring to the outage, stated that "we got this wrong" and that it is "super important to own it when you do things horribly wrong, which we did in this case." (*Id.* at 66). Shawn Henry, a CrowdStrike executive, wrote in a public apology on behalf of CrowdStrike that "on Friday we failed you." (*Id.*). Defendant Kurtz called the outage a "transformational event" for the company. (*Id.* at 80). According to Plaintiffs, these statements strengthen the scienter inference.

[29] It is true that there are "special circumstances" that would permit a plaintiff to plead scienter by pleading a defendant's company in the position. *Neiman*, 854 F.3d at 749–750. The "special circumstances" exception does not apply in the instant case, as CrowdStrike is a large company, the transaction at issue—an update to the Falcon sensor that occurs many times daily—was not "critical to the company's vitality," and Defendants' statements were not "internally inconsistent with one another." *See id.* (quoting *Local 731 I.B. of T. Excavators & Pavers Pension Trust Fund v. Diodes, Inc.*, 810 F.3d 951, 959 (5th Cir. 2016)).

Defendants argue in their motion to dismiss that these statements are not admissions of scienter, as Defendants do not admit in these post-outage statements that any alleged misrepresentations were false or misleading when made. Rather, Defendants contend that Plaintiffs' argument is a "classic fraud-by-hindsight pleading," and that promising corrective measures is not proof of what Defendants knew at the time the alleged misrepresentations were made. (Mot. to Dismiss, Dkt. 47, at 36–37). Plaintiffs respond that this is "not mere 'fraud by hindsight'" because how "quickly and easily [CrowdStrike] implemented the industry-standard testing and release protocols they previously lacked" demonstrates that Defendants knew they were being reckless. (Pls.' Resp., Dkt. 48, at 37–38).

As to the CrowdStrike executives' post-outage statements acknowledging their mistakes, Fifth Circuit precedent forecloses such statements, standing alone, as leading to a strong inference of scienter. The Fifth Circuit wrote in *Tuchman*:

> The plaintiffs' complaint recites various episodes and **acknowledgements of corporate mismanagement** and failings of quality control. . . . However, corporate mismanagement does not, standing alone, give rise to a 10b–5 claim, and **mea culpa does not sufficiently satisfy the scienter requirements of pleading in securities fraud cases unless it is shown to relate to activities that have a definable nexus or relationship with the sale or purchase of a security**.

Tuchman, 14 F.3d at 1070 (emphasis added). Here, Plaintiffs do not connect CrowdStrike's admissions of "mea culpa" to the sale or purchase of a security. Their apologies and acknowledgments of fault made with hindsight therefore do not lead to a strong inference of scienter. Moreover, unlike in *Lormand*, the post-outage apologies and admissions of fault in this case do not shed light on Defendants' states of mind prior to the July 2024 outage. *See Lormand*, 565 F.3d at 254 (holding that post-outage admissions by the defendants were evidence of scienter where the admissions "directly and cogently tend[ed] to prove [the defendants'] state-of-mind at the time of their misleading statements and omissions").

As to CrowdStrike's alleged "quick[] and easy[]" implementation of industry standards for Rapid Response Content updates, the Court finds that this only leads to a slight inference of scienter. It is possible that CrowdStrike quickly changing their testing and roll-out processes of Rapid Response Content updates is a sign that software engineers at CrowdStrike knew something was wrong with their prior protocols, were aware of exactly how to fix it, but had been directed by Defendants to not implement industry-standard protocols.

The Court finds, however, that the more plausible opposing inference is that CrowdStrike's software engineers could quickly and easily implement standard testing procedures for Falcon sensor updates because they were already doing such testing for other software and/or code updates.[30] The Court has reached this conclusion in light of the specified purpose behind Rapid Response Content updates. As Plaintiffs themselves acknowledge in their Complaint:

> Falcon's **automatic "updates" were a centerpiece of its value proposition to both customers and investors**. According to CrowdStrike, the Falcon platform was uniquely suited to protect its customers because CrowdStrike issued regular, **automatic "updates" that incorporated real-time data into the Falcon platform that helped secure its customers' computers**.
>
> CrowdStrike called this remote update system "Rapid Response." **The Rapid Response updates were central to CrowdStrike's investment thesis, as CrowdStrike claimed that its Rapid Response system made its Falcon cybersecurity threat detection software better than its competitors.** CrowdStrike emphasized that the Rapid Response updates were "reliable" and "secure," with the Company telling customers and investors alike that its "software development methodology that allows for rapid, frequent, and reliable code updates" and replaces "manual, legacy methods of deploying code to ensure faster and more secure updates."

(Compl., Dkt. 41, at 13) (emphasis added). In other words, Rapid Response Content updates were a significant part of what made CrowdStrike's Falcon software unique in a market filled with

[30] Plaintiffs themselves claim that the "software development testing, quality assurance, and rollout processes that CrowdStrike failed to conduct are not complex . . . ." (Compl., Dkt. 41, at 59). This allegation by Plaintiffs further strengthens a nonfraudulent inference and weakens Plaintiffs' argument that Defendants' ability to quickly apply industry standards to Rapid Response Content updates suggests scienter.

competitors. In the absence of other "specific facts" alleged that support a strong inference of scienter, *see Flaherty & Crumrine Preferred Income Fund, Inc. v. TXU Corp.*, 565 F.3d 200, 213 (5th Cir. 2009), the Court finds an opposing, nonfraudulent inference more probable—that Defendants treated Rapid Response Content updates differently than other types of software or code because doing so enabled them to implement "automatic" updates based on "real-time data" in a way that no other competitor was doing. *See Tellabs*, 551 U.S. at 314 (holding that a strong inference of scienter must be "at least as compelling as any opposing inference of nonfraudulent intent"). Defendants' post-outage statements acknowledging fault with the benefit of hindsight do not change that the stronger inference is the nonfraudulent one.

d. Miscellaneous Scienter Allegations

Plaintiffs also make a number of miscellaneous allegations that they claim support a strong inference of scienter. The Court will review these allegations holistically to determine whether they lead to a strong inference of scienter. *See Owens*, 789 F.3d at 536–37.

- Falcon was CrowdStrike's only product, so Defendants knew or were severely reckless in not knowing about the Company's failure to properly test and roll out Falcon updates. (Compl., Dkt. 41, at 55).

- Defendants Kurtz and Sentonas "repeatedly touted CrowdStrike's software testing." (Compl., Dkt. 41, at 55–56).[31]

- Defendants assured investors that the software does not result in blue screens. (Compl., Dkt. 41, at 56).

- Defendants Kurtz and Sentonas previously were Chief Technology Officers at McAfee, another cybersecurity company. While at McAfee, the company released a faulty software update that caused computers to blue screen. The incident allegedly could have been prevented by testing the update in a pre-production environment. According to Plaintiffs, Defendant Kurtz told CrowdStrike investors that he had "learned this lesson" at McAfee. Industry experts later compared the McAfee and CrowdStrike outages as similar. (Compl., Dkt. 41, at 57–58).

[31] As discussed in Section III(B)(3), *supra*, multiple of the alleged misstatements regarding software testing were severely taken out of context.

- CrowdStrike violated industry standards governing software development, even though "Defendants held themselves out as knowledgeable of the basic tenets of safe software update development and release." (Compl., Dkt. 41, at 59–60).

- CrowdStrike's lack of a quality assurance team was "obvious and known." (Compl., Dkt. 41, at 60).

- CrowdStrike executives, "including Defendants Kurtz and Sentonas," certified in sworn declarations that CrowdStrike met FedRAMP requirements.

Viewing these scienter allegations and the previously discussed scienter allegations as a whole, the Court holds that these allegations do not lead to a strong inference of scienter. They remain less persuasive than the compelling inference that Rapid Response Content updates were treated differently by Defendants' software engineers due to their automatic nature, rather than them being treated differently for a fraudulent or severely reckless reason.

For instance, regarding Defendant Sentonas's assurance that Falcon does not cause endpoints to blue screen, these statements were "reasonably consistent with reasonably available data" at that time, as Falcon updates had not yet caused computers to blue screen. Defendants were not required to provide an "overly gloomy" warning that their software may cause blue screens. *See Abrams*, 292 F.3d at 433 ("[A]s long as public statements are reasonably consistent with reasonably available data, corporate officials need not present an overly gloomy or cautious picture of the company's current performance.").

As to Plaintiffs' allegation that Defendants knowingly violated industry standards, mere noncompliance with industry standards, without plausible allegations about the defendant's intent, are also not sufficient to plead a strong inference of scienter. *See Shaw Grp.*, 537 F.3d at 534 (citation omitted) (noting that the Fifth Circuit has repeatedly held that failure to follow accounting standards, without more, does not establish scienter). And, regardless, the Court finds a more plausible inference to be that industry standards were thought to be inapplicable to Rapid Response Content updates, as they were a novel type of update in the cybersecurity industry whose value was based on them being implemented automatically, rather than them being slowed down by normal testing and roll-out processes. The fact that Defendants determined—with hindsight—that less rigorous testing was a bad decision is not a basis for securities fraud.

Regarding Defendants' FedRAMP sworn declarations, the Court first notes that Plaintiffs fail to offer specific facts alleging that Defendants Kurtz or Sentonas themselves signed the FedRAMP verifications.[32] And, regardless, even if they had signed the FedRAMP verifications, Plaintiffs have failed to plausibly allege that Defendants Kurtz or Sentonas "knew or were severely reckless in not knowing that any statement in the [FedRAMP] certifications was false or misleading." *See Heck v. Orion Grp. Holdings, Inc.*, 468 F. Supp. 3d 828, 855 (S.D. Tex. 2020). As the Court explained in Section III(B)(4), the part of NIST standard AC-5 that mentions a separate team performing quality assurance could reasonably be interpreted as requiring a separate quality assurance team, *or* it could reasonably be interpreted as a separate quality assurance team being a mere example of how software development teams could be organized. Without more information on how this standard has been interpreted in the past, Plaintiffs have not plausibly alleged that Defendants Kurtz or Sentonas knew or should have known that CrowdStrike was violating AC-5 by not having a separate quality assurance team. Overall, these allegations are not enough to contribute to a strong inference of scienter.

3. Defendants Kurtz and Sentonas' Knowledge of Unattributed Website Statements

"To plead scienter for unattributed corporate statements, a plaintiff must first tie the statement to 'a corporate officer who can be seen as acting on behalf of the corporation in making the statement.'" *In re Plains All Am. Pipeline*, 307 F. Supp. 3d. 583, 627 (S.D. Tex. 2018) (quoting *In re*

[32] FE-8 alleges that "Defendant Kurtz, or someone else in CrowdStrike's C-Suite, including Defendant Sentonas had to sign certifications attesting to CrowdStrike's compliance with these requirements." (Compl., Dkt. 41, at 61). Such a vague allegation does not satisfy the heightened pleading standard from Federal Rule of Civil Procedure 9(b) to allege "who, what, when, where, and how." *See Owens*, 789 F.3d at 535 (citing *ABC Arbitrage Plaintiffs Grp.*, 291 F.3d at 349–50).

BP p.l.c. Sec. Litig., 843 F. Supp. 2d at 789). Additionally, in certain circumstances, a corporate executive may be considered as "making" a statement for purposes of Rule 10b-5 if they were the person "with ultimate control over the statement." *Janus Cap. Grp., Inc. v. First Derivative Traders*, 564 U.S. 135, 142 (2011).

Defendants stress that four of the alleged misstatements in Plaintiffs' Complaint were published on CrowdStrike's website and that Plaintiffs failed to plead particularized facts demonstrating that Defendants Kurtz or Sentonas made, approved, or were aware of these statements. (Mot. to Dismiss, Dkt. 47, at 39). Plaintiffs argue in their response that this case is similar to *In re SolarWinds Corporation Securities Litigation*, 595 F. Supp. 3d 573 (W.D. Tex. 2022), in which this Court found that the plaintiffs had sufficiently pleaded that corporate executives had "made" statements on the company's website. (Pls.' Resp., Dkt. 48, at 42). In *SolarWinds*, the defendants were explicitly alleged to have "reviewed and approved" the company's "Security Statement" statement being challenged as misleading. *Id.* at 586. Additionally, one of the defendant's photos was included with the statement, and he was alleged to be "the face (literally)" of the cybersecurity statement. *Id.* at 584, 586. That same defendant also frequently did interviews about the company's cybersecurity and was alleged to "address[] cybersecurity issues when they arose." *Id.* at 584.

In this case, however, there are no particular allegations connecting Defendants Kurtz or Sentonas to the specific alleged misstatements at issue. One of the alleged misstatements (about phased rollouts) on the website is from a blog post about JSON marshaling; two of the alleged misstatements are about compliance with FedRAMP and DoD requirements; and a fourth alleged misstatement (about software testing protocols) is from an article about a certain software development methodology. (Compl., Dkt. 41, at 76–78). As to the statements in the JSON marshaling blog post and CI/CD article, there are no allegations in the Complaint supporting that

Defendants Kurtz or Sentonas directly reviewed and approved their software engineers' technical blog posts and articles or were closely involved in those areas of their engineers' work.[33] Similarly, *none* of the statements about FedRAMP or DoD requirements in Plaintiffs' entire Complaint come from either Defendant Kurtz or Sentonas. And Plaintiffs only vaguely allege that "Defendant Kurtz, or someone else in CrowdStrike's C-Suite, including Defendant Sentonas had to sign certifications attesting to CrowdStrike's compliance with these requirements." (Compl., Dkt. 41, at 61). This is nowhere close to the alleged level of involvement in *SolarWinds*, and it is not enough to attribute the website's FedRAMP and DoD compliance statements to Defendants Kurtz and Sentonas in particular.

Overall, unlike in *SolarWinds*, where one of the defendants was alleged to be "the face (literally)" of the cybersecurity statement at issue, to frequently do interviews about the company's cybersecurity, and to "address[] cybersecurity issues when they arose," *In re SolarWinds*, 595 F. Supp. 3d at 584, neither Defendant Kurtz nor Sentonas[34] were alleged to be "the face" of Rapid Response Content updates, to frequently do interviews about Rapid Response Content updates, or to be the one addressing issues with Rapid Response Content updates when they arose. Plaintiffs therefore fail to sufficiently plead that Defendants Kurtz or Sentonas "made" any of the alleged misstatements on the CrowdStrike website.[35]

[33] It is not enough for Plaintiffs to plead that Defendants Kurtz and Sentonas "reviewed, approved, and controlled the contents" of CrowdStrike's website based on FE-8's vague claim that she saw them "specifically direct[] that certain information be published on CrowdStrike's website." (Compl., Dkt. 41, at 75 & n.179).

[34] In fact, not a single alleged misstatement attributed to Defendant Sentonas by Plaintiffs was about software testing.

[35] Because Plaintiffs did not allege that the individual employees who wrote the JSON marshaling blog post and CI/CD article acted with scienter, the Court does not consider whether CrowdStrike itself could be liable for those statements. *See Southland Sec. Corp.*, 365 F.3d at 367 (holding that, because the complaint did not assert that any particular employee *other than* the named defendants acted with scienter, the court need only consider the state of mind of the named defendants when determining whether the pleaded facts give rise to a strong inference that the company itself had the requisite scienter).

4. Collective Impact of Scienter Allegations

Ultimately, read together, Plaintiffs' scienter allegations do not create an inference as strong as the opposing inference of nonfraudulent intent provided by Defendants. *See Alaska Elec. Pension Fund*, 915 F.3d at 982 (quoting *Tellabs*, 551 U.S. at 314) ("To withstand a motion to dismiss, 'an inference of scienter must be more than merely plausible or reasonable—it must be cogent and at least as compelling as any opposing inference of nonfraudulent intent.'"). In summary, based on (1) Defendants explicitly promoting Rapid Response Content updates being automatic and done in real time; (2) investors allegedly valuing the uniqueness of Rapid Response Content updates being automatic and done in real time; (3) Defendants disclosing the risk that the "adverse effects of any service interruptions . . . may be disproportionately heightened due to the nature of [CrowdStrike's] business and the fact that [its] customers have a low tolerance for interruptions of any duration";[36] (4) Plaintiffs' failure to plausibly allege a motive for fraud; and (5) Plaintiffs' failure to plausibly allege strong circumstantial evidence of fraud or severe recklessness, Plaintiffs have failed to plausibly plead a strong inference of scienter for the individual Defendants or for CrowdStrike itself.[37] Thus, even though the Court found in Section III(B), *supra*, that Plaintiffs had plausibly alleged two misleading statements, the Court will grant Defendants' motion to dismiss.

D. Section 20 Claims

Control person liability under Section 20(a) of the Exchange Act, codified at 15 U.S.C. § 78t(a), requires an underlying violation of the Exchange Act. *R2 Inv. LDC v. Phillips*, 401 F.3d 638, 641 (5th Cir. 2005). Because Plaintiffs have failed to plausibly plead a primary violation of Section

[36] *See Owens*, 789 F.3d at 540 (noting that disclosure of risks weighs against scienter).

[37] Regarding CrowdStrike's scienter, the Court does not find a strong inference of corporate scienter either through statements made by Defendants Kurtz or Sentonas or through unattributed statements "so dramatic 'it would have been approved by corporate officials sufficiently knowledgeable about the company to know that the announcement was false." *See In re Dell Inc., Sec. Litig.*, 591 F. Supp. 2d at 899 (W.D. Tex. 2008) (first citing *Southland Sec. Corp.*, 365 F.3d at 366; and then quoting *Makor Issues & Rights, Ltd. v. Tellabs, Inc.*, 513 F.3d 702, 710 (7th Cir. 2008)).

10(b) of the Exchange Act and Rule 10b-5, the Court also dismisses Plaintiffs' Section 20(a) claims against Defendants Kurtz and Sentonas.

E. Leave to Amend

Plaintiff requests leave to amend should the Court grant in part or in whole Defendants' motion. (Pls.' Resp., Dkt. 48, at 42). Defendants' Reply does not respond to this request other than asking that this case be dismissed with prejudice. (Defs.' Reply, Dkt. 55, at 22).

Given the "bias in favor of granting leave to amend" in this Circuit, *Lyn-Lea Travel Corp. v. Am. Airlines, Inc.*, 283 F.3d 282, 286 (5th Cir. 2002), the Court will allow Plaintiff to file a motion for leave to file an amended pleading. The motion must include as attachments the proposed amended pleading, as well as a redlined version of the proposed amending pleading showing the differences between it and the Complaint, (Dkt. 41).

IV. CONCLUSION

For the reasons given above, **IT IS ORDERED** that Defendants' Motion to Dismiss Plaintiff's Consolidated Class Action Complaint, (Dkt. 47), is **GRANTED**, such that Plaintiff's claims are dismissed in their entirety without prejudice.

IT IS FURTHER ORDERED that Plaintiff may file a motion for leave to file an amended pleading on or before **January 26, 2026**. If Plaintiff chooses to file a motion for leave to file an amended pleading, Plaintiff shall attach to the motion (1) a proposed amended pleading and (2) a redlined document showing the differences between the proposed amended pleading and Plaintiff's Complaint, (Dkt. 41).

SIGNED on January 12, 2026.

ROBERT PITMAN
UNITED STATES DISTRICT JUDGE