UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

DOYUN KIM,

Plaintiff,

v.

ADVANCED MICRO DEVICES, INC., et al.,

Defendants.

Case No. 5:18-cv-00321-EJD

ORDER GRANTING MOTION TO DISMISS

Re: Dkt. No. 38

Plaintiffs bring this putative class action against Advanced Micro Devices, Inc. ("AMD"), its CEO Lisa T. Su, and its CFO Devinder Kumar (collectively with AMD "Defendants") for allegedly making misleading statements or omissions relating to the Spectre computer vulnerabilities. Plaintiffs allege that Defendants violated Section 10(b) of the Exchange Act and of Rule 10b-5 and Su and Kumar individually violated Section 20(a) of the Exchange Act all to artificially inflate AMD's stock prices. Plaintiffs seek to represent a class of individuals who purchased AMD's stock at the allegedly inflated prices between June 29, 2017 and January 11, 2018 (the "Class Period"). Presently before the Court is Defendants' motion to dismiss. Pursuant to Civil Local Rule 7-1(b), the Court has taken the motion under submission without oral argument. Having considered the parties' papers, the Court now grants the motion and provides Plaintiffs with leave to amend.

I. Background

AMD is a publicly traded manufacturer of processors that are integral to desktop and laptop computers, mobile devices, and server processors. Amended Class Action Complaint ("ACAC") ¶¶ 2-3, 20-21. These processors are integrated circuits that form the central processing

units ("CPUs") of computers. *Id.* ¶ 23. AMD competes with other processor manufacturers, like Intel and ARM Holdings. *Id.* ¶ 24. Over the course of 2017, AMD's total revenue increased by 25 percent—over $1.05 billion. *Id.* ¶ 26. This growth was driven in large part by the success of its Ryzen processors, which were launched in March of that year. *Id.* ¶¶ 27-30.

Microprocessors, like other hardware or software, can be subject to "vulnerabilities." *See id.* ¶ 35. A "vulnerability" is a weakness in a computer system that can be exploited by a bad actor to obtain access to the computer system. *Id.* A vulnerability exists from the time that weakness is introduced to or discovered in deployed computer systems until it is removed or patched. *Id.* This matter concerns two vulnerabilities known as Spectre Variant 1 and Spectre Variant 2 that were present on AMD's processors. *Id.* ¶ 6. Another vulnerability known as Meltdown was discovered and became public at the same time as the Spectre vulnerabilities. *Id.* ¶ 61. AMD's processors were not susceptible to Meltdown. *Id.* In theory, a bad actor could exploit the Spectre vulnerabilities to gain access to areas of an affected computer's memory. *Id.* ¶ 41. In particular, the bad actor could access the computer's "kernel," a central part of the operating system that connects software with the CPU and other hardware. *Id.* The kernel prevents programs or applications from reading or accessing data in other programs or applications. *Id.* The bad actor could exploit Spectre with an innocuous appearing program to gain access to the data and memory in other programs. *Id.* ¶43. In other words, the bad actor could gain access to personal or private information stored in the computer's memory, such as credit card information, passwords, etc. *Id.* ¶ 43. The bad actor though would not be able to alter anything on the computer. *Id.*

In 2014, Google established a fulltime security team known as Project Zero to search for potential vulnerabilities in publicly deployed computer systems. *Id.* ¶ 37. When Project Zero discovers a vulnerability, it will notify the companies responsible for the vulnerability before publicly disclosing it. *Id.* ¶¶ 38-39. This way, the affected companies can address and eliminate the vulnerability before public disclosure alerts bad actors. *Id.* ¶¶ 38-40. Project Zero has modified its public disclosure policy to ensure the vulnerability remains secret while the affected company works on patches and/or updates to fix the vulnerability. *Id.* ¶ 40.

On June 1, 2017, Project Zero informed AMD that it had discovered Spectre Variant 1 on its processors. *Id.* ¶¶ 41, 47. Project Zero did not state that it had observed Spectre Variant 2 on AMD's processors. *Id.* ¶ 45. At the same time, Project Zero alerted other processor manufacturers that were susceptible to Spectre and/or Meltdown. *Id.* 41. Keeping with Project Zero's usual practice, it did not publicly disclose these vulnerabilities. *Id.* ¶ 47. AMD would later represent that after receiving Project Zero's report, it "engaged across the [technology] ecosystem to address [Project Zero's] findings." *Id.* ¶ 58.

On July 25, 2017, Defendants filed with the SEC a Form 8-K that incorporated the risk disclosure from the Form 10-Q that AMD had filed on May 8, 2017. *Id.* ¶¶ 51-52. The risk disclosure statement read, in relevant part:

> ***Data breaches and cyber-attacks could compromise our intellectual property or other sensitive information, be costly to remediate and cause significant damage to our business and reputation.***
>
> In the ordinary course of our business, we maintain sensitive data on our networks, including our intellectual property and proprietary or confidential business information relating to our business and that of our customers and business partners. The secure maintenance of this information is critical to our business and reputation. We believe that companies have been increasingly subject to a wide variety of security incidents, cyber-attacks, hacking and phishing attacks, and other attempts to gain unauthorized access. These threats can come from a variety of sources, all ranging in sophistication from an individual hacker to a state-sponsored attack. Cyber threats may be generic, or they may be custom-crafted against our information systems. Cyber-attacks have become increasingly more prevalent and much harder to detect and defend against. Our network and storage applications, as well as those of our customers, business partners, and third party providers, may be subject to unauthorized access by hackers or breached due to operator error, malfeasance or other system disruptions. It is often difficult to anticipate or immediately detect such incidents and the damage caused by such incidents. These data breaches and any unauthorized access, misuse or disclosure of our information or intellectual property could compromise our intellectual property and expose sensitive business information. ***Cyber-attacks on us or our customers, business partners or third party providers could also cause us to incur significant remediation costs, result in product development delays, disrupt key business operations and divert attention of management and key information technology resources.*** These incidents could also subject us to liability, expose us to significant expense and cause significant harm to our reputation and business. ***In addition, we could be subject to potential claims for damages resulting from***

> ***loss of data from alleged vulnerabilities in the security of our processors.***

Id. ¶ 52 (emphasis in the ACAC). On August 3, 2017, Defendants filed AMD's quarterly Form 10-Q that contained a risk disclosure identical to the one in the May 2017 Form 10-K. *Id.* ¶ 54. On November 2, 2017, Defendants filed another Form 10-Q. *Id.* ¶ 56. The risk disclosure in this filing was identical to the previous risk disclosures, except for adding one phrase, which is not relevant to this motion, to the second sentence. *Id.*

Project Zero publicly disclosed the existence of the Spectre and Meltdown vulnerabilities on January 3, 2018. *Id.* ¶ 41. That same day, a group of independent researchers published their own report on the vulnerabilities (the "Kocher Report"). *Id.* The Kocher Report stated that the researchers had observed Spectre Variant 2 on AMD's processors, and that AMD's Ryzen processors were susceptible to both Spectre Variants. *Id.* ¶ 46. These reports confirmed that processors made by AMD, Intel, and ARM Holdings were susceptible to Spectre and/or Meltdown. *Id.* ¶ 44. Meltdown did not impact AMD's processors. *Id.*

That day, AMD posted a message to its website that read:

> There has been recent press coverage regarding a potential security issue related to modern microprocessors and speculative execution. Information security is a priority at AMD, and our security architects follow the technology ecosystem closely for new threats.
>
> It is important to understand how the speculative execution vulnerability described in the research relates to AMD products, but please keep in mind the following:
>
> • The research described was performed in a controlled, dedicated lab environment by a highly knowledgeable team with detailed, non-public information about the processors targeted.
>
> • The described threat has not been seen in the public domain.
>
> When AMD learned that researchers had discovered a new CPU attack targeting the speculative execution functionality used by multiple chip companies' products, we immediately engaged across the ecosystem to address the teams' findings.
>
> The research team identified three variants within the speculative execution research. The below grid details the specific variants detailed in the research and the AMD response details.

Id. ¶ 58. The posting further provided the following details for each vulnerability:

- For Spectre Variant 1: "Resolved by software / OS updates to be made available by system vendors and manufacturers. Negligible performance impact expected." *Id.*
- For Spectre Variant 2: "Differences in AMD architecture mean ***there is a near zero risk of exploitation*** of this variant. Vulnerability to Variant 2 has not been demonstrated on AMD processors to date." *Id.* (emphasis in the ACAC).
- For Meltdown: "Zero AMD vulnerability due to AMD architecture differences." *Id.*

Also on January 3, 2018, an AMD spokesperson told investors Variant 2 posed a "near zero risk" to AMD's processors. *Id.* ¶ 59. That day, AMD's stock price rose from its January 2, 2018 close of $10.98 to a January 3, 2018 close of $11.55. *Id.* ¶ 61.

On January 8, 2018, Su appeared on the cable TV station CNBC for an interview, where she said, in part, the following:

> Su: [M]oving to the other security conversation around Spectre, you know this one is actually a little broader. You know it does affect our processors as well as others. There are a couple variants in there. The first variant is one that we believe, as an industry, we're doing a very good job in coming together. And so the operating system vendors are actually putting some mitigations in place. And that, we think, is a strong solution.
>
> CNBC Host: And that's the one where people are concerned about how much you might have to throttle the processor in order to make it safe. There were some initial reports out that it might be as much as 30% from some applications, but Apple and others seem to be saying, hey don't worry, it won't be that much.
>
> Su: Yeah, and I think some of those numbers are around Meltdown. Some of them were around Spectre. But to be fair, I think it's very application dependent and very processor dependent. And so I do believe that there are good mitigations in place. I do believe that there are some workloads that you might see larger performance variance. But on this particular Spectre one, we feel that the performance will be small.
>
> CNBC Host: And the second Spectre variant?
>
> Su: And the second Spectre variant is one that, again, due to some of our architectural differences, from and AMD side, ***we think it's rare***. I think, we think, it's difficult to access, you know, out in real world applications. But, I got to tell you, John, I said security is job one for us. We're being very vigilant. We are working with all of our partners. And we're going to continue to, you know, watch this space as it goes forward.

Id. ¶ 62 (emphasis in the ACAC). That day, AMD's stock rose from $12.01 at opening to $12.28 at close. *Id.* ¶ 63.

Plaintiffs assert that Defendants "reveal[ed] the truth" that AMD's processors were susceptible to Variant 2 on January 11, 2018. *Id.* ¶ 65. Defendants issued a post-market press release with the title "An Update on AMD Processor Security." *Id.* The press release represented:

> The public disclosure on January 3rd that multiple research teams had discovered security issues related to how modern microprocessors handle speculative execution has brought to the forefront the constant vigilance needed to protect and secure data. These threats seek to circumvent the microprocessor architecture controls that preserve secure data.
>
> At AMD, security is our top priority and we are continually working to ensure the safety of our users as new risks arise. As a part of that vigilance, I wanted to update the community on our actions to address the situation.
>
> - ***Google Project Zero (GPZ) Variant 1 (Bounds Check Bypass or Spectre) is applicable to AMD processors.***
>
> - We believe this threat can be contained with an operating system (OS) patch and we have been working with OS providers to address this issue.
>
> - Microsoft is distributing patches for the majority of AMD systems now. We are working closely with them to correct an issue that paused the distribution of patches for some older AMD processors (AMD Opteron, Athlon and AMD Turion X2 Ultra families) earlier this week. We expect this issue to be corrected shortly and Microsoft should resume updates for these older processors by next week. For the latest details, please see Microsoft's website.
>
> - Linux vendors are also rolling out patches across AMD products now.
>
> - ***GPZ Variant 2 (Branch Target Injection or Spectre) is applicable to AMD processors.***
>
> - While we believe that AMD's processor architectures make it ***difficult to exploit Variant 2, we continue to work closely with the industry on this threat***. We have defined ***additional steps through a combination of processor microcode updates and OS patches that***

we will make available to AMD customers and partners to further mitigate the threat.

- AMD will make optional microcode updates available to our customers and partners for Ryzen and EPYC processors starting this week. We expect to make updates available for our previous generation products over the coming weeks. These software updates will be provided by system providers and OS vendors; please check with your supplier for the latest information on the available option for your configuration and requirements.

- Linux vendors have begun to roll out OS patches for AMD systems, and we are working closely with Microsoft on the timing for distributing their patches. We are also engaging closely with the Linux community on development of "return trampoline" (Retpoline) software mitigations.

Id. (emphasis in the ACAC). That day, Su gave an interview to Yahoo Finance, during which she said: "to clarify, for Meltdown, AMD is not susceptible . . . we don't have a susceptibility to that variant. But with Spectre, AMD is susceptible," and "[w]e will have some micro-code and some updates with our software partners to ensure that [Spectre] Variant 2 is taken care of. We want to make sure these patches are rolled out as smoothly as possible. We did have an issue with some of the older processors with Microsoft and their patch. We're working on that in real-time, and we expect that to be cleared up very shortly." *Id.* ¶ 66. That day, AMD's stock fell 0.99 percent, from $12.24 to $12.02. *Id.* ¶ 68.

Plaintiffs do not allege that Spectre was ever successfully exploited on any AMD processors—or on any other manufacturer's processors—in publicly deployed computers. Nor do Plaintiffs allege that Defendants ever believed, or had reason to believe that a successful exploitation of Spectre was imminent or likely.

II. Request for Judicial Notice

Defendants ask the Court to take judicial notice of 15 separate documents. Dkt. 39, Req. for Judicial Notice. Plaintiffs oppose the request. Dkt. 41, Opp'n to Req. for Judicial Notice; Opp'n at 14-15. Courts may take judicial notice of an adjudicative fact that is "not subject to reasonable dispute," meaning that it is "generally known" or "can be accurately and readily

determined from sources whose accuracy cannot reasonably be questioned." Fed. R. Evid. 201(b). The Ninth Circuit has recently cautioned that when district courts take judicial notice of a document, they must "consider—and identify—which fact or facts it is noticing from [the document]. Just because the document itself is susceptible to judicial notice does not mean that every assertion of fact within that document is judicially noticeable for its truth." *Khoja v. Orexigen Therapeutics, Inc.*, 899 F.3d 988, 999 (9th Cir. 2018).

The Court takes judicial notice of AMD's historic stock prices during January 2018 contained in Exhibit 2. Dkt. 39-3, Ex. 2 to the Decl. of Matthew W. Close ("Ex. 2"). Courts may take judicial notice of historical stock prices because they are "subject to accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned." *Brodsky v. Yahoo! Inc.*, 630 F. Supp. 2d 1104, 1111-12 (9th Cir. 2009); *cf. Khoja*, 899 F.3d at 1001. The facts of AMD's stock prices in January 2018 do not contradict any factual allegations in the Amended Complaint, and Plaintiffs do not contest the authenticity or accuracy of Exhibit 2. *See Khoja*, 899 F.3d at 1001.

Because the Court does not presently consider any of the other documents in Defendants' request for judicial notice, the Court DENIES the remainder of request without prejudice.

III. Legal Standard

A complaint must include "a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). "To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face; that is, plaintiff must plead factual content that allows the court to draw the reasonable inference that the defendant is liable." *Khoja*, 899 F.3d at 1008 (internal quotations, citations, and alterations omitted). When "faced with a Rule 12(b)(6) motion to dismiss a [Section] 10(b) action, courts must . . . accept all factual allegations in the complaint as true." *Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 322 (2007). But, courts "do not, however, accept as true allegations that are conclusory." *In re NVIDIA Corp. Sec. Litig.*, 768 F.3d 1046, 1051 (9th Cir. 2014). "Factual allegations must be enough to raise a right to relief above the speculative level." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007).

In addition, Section 10(b) claims are subject to the heightened pleading standards of Rule 9(b) and the Private Securities Litigation Reform Act of 1995 ("PSLRA"). *Tellabs*, 551 U.S. at 313. Rule 9(b) requires the plaintiff "state with particularity the circumstances constituting fraud." A plaintiff must, therefore, "set forth what is false or misleading about a statement, and why it is false." *Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1106 (9th Cir. 2003). The "PSLRA imposes additional specific pleading requirements, including requiring plaintiffs to state with particularity both the facts constituting the alleged violation and the facts evidencing scienter." *In re Rigel Pharm., Inc. Sec. Litig.*, 697 F.3d 869, 876 (9th Cir. 2012).

III. Section 10(b) of the Exchange Act and Rule 10b-5

Plaintiffs contend that Defendants violated Section 10(b) of the Exchange Act and Rule 10b-5 by making several allegedly misleading statement or omissions related the Spectre vulnerabilities. The ACAC raises three categories of allegedly misleading statements or omissions: (1) risk disclosures in corporate filings during the class period, (2) marketing statements from the launch of the Ryzen processor, and (3) public statements made in January 2018 concerning the disclosure of the Spectre and Meltdown vulnerabilities. But in their opposition, Plaintiffs abandon their claim to the extent it is based on the representations from the launch of the Ryzen processors. The Court therefore dismisses this claim as far as it relies on those representations. *See Norfolk Cty. Ret. Sys. v. Solazyme, Inc.*, 2018 WL 3126393, at *10 (N.D. Cal. June 26, 2018); *Qureshi v. Countrywide Home Loans, Inc.*, 2010 WL 841669, at *7 n.2 (N.D. Cal. Mar. 10, 2010). To plead a claim for violations of Section 10(b) of the Exchange Act and Rule 10b-5, a plaintiff must allege facts showing (1) a material misrepresentation or omission, (2) scienter, (3) a connection between the misrepresentation or omission and the purchase or sale of a security; (4) reliance; (5) economic loss; and (6) loss causation. *NVIDIA*, 768 F.3d at 1052. Defendants argue that that the ACAC fails to adequately plead the first two elements.

A. Material Misrepresentation or Omission

To adequately plead a material misrepresentation, a plaintiff must specify "[1] each statement alleged to have been misleading, [2] the reason or reasons why the statement is misleading, and, [3] if an allegation regarding the statement or omission is made on information

and belief, the complaint shall state with particularity all facts on which that belief is formed." *Khoja*, 899 F.3d at 1008 (quoting 15 U.S.C. § 78u-4(b)(1)). The allegedly misleading statements must "directly contradict what the defendant knew at that time." *Id.* Statements that are not false, but that omit material information may be misleading if the defendant had a duty to disclose. *Id.* The "duty to disclose does not arise from the mere possession of nonpublic market information." *In re Verity, Inc. Sec. Litig.*, 2000 WL 1175580, at *4 (N.D. Cal. Aug. 11, 2000) (citing *Chiarella v. United States*, 445 U.S. 222, 235 (1980)). But, "[d]isclosure is required . . . only when necessary to make statements made, in light of the basic circumstances under which they were made, not misleading." *Flynn v. Sientra, Inc.*, 2016 WL 3360676, at *10 (C.D. Cal. June 9, 2016) (quoting *Maxtrixx Initiatives, Inc. v. Siracusano*, 563 U.S. 27, 44 (2011) (internal alteration and quotation omitted)). An omission is misleading where it "affirmatively create an impression of a state of affairs that differs in a material way from the one that actually exists." *Id.* (quoting *Brody v. Transitional Hosps. Corp.*, 280 F.3d 997, 1006 (9th Cir. 2002)).

1. The Risk Disclosure Statements

Plaintiffs allege that three of AMD's SEC filings are materially false or misleading because their risk disclosure statements omit any reference to Spectre. ACAC ¶¶ 51, 52, 54, 56. The risk disclosure statements read in part:

> Data breaches and cyber-attacks could compromise our intellectual property or other sensitive information, be costly to remediate and cause significant damage to our business and reputation. . . . Cyber-attacks on us or our customers, business partners or third party providers could also cause us to incur significant remediation costs, result in product development delays, disrupt key business operations and divert attention of management and key information technology resources. These incidents could also subject us to liability, expose us to significant expense and cause significant harm to our reputation and business. In addition, we could be subject to potential claims for damages resulting from loss of data from alleged vulnerabilities in the security of our processors.

Id.

Plaintiffs allege that this statement is false and misleading because Defendants knew at the time that AMD's chips were susceptible to Spectre, "leaving the owners of [AMD's] chips in

danger of having their personal and confidential information misappropriated." *Id.* ¶¶ 53, 55, 57. They further allege that Defendants "knew that AMD would necessarily incur additional costs to develop and distribute patches to allow its users to guard against the Spectre vulnerability. *Id.* They argue that by raising the danger of cyber attacks and data breaches to their processors in the risk disclosure statements, Defendants took on a duty to fully disclose the risk posed by Spectre. Opp'n at 6-7. This omission presented reasonable investors with "the impression of a state of affairs . . . that differed materially from the one that actually existed," they argue. *Sec. & Exch. Comm'n v. Strategic Glob. Investments, Inc.*, 262 F. Supp. 3d 1007, 1018 (S.D. Cal. 2017). Risk disclosures may be actionable "as material omissions when the disclosures speak to entirely . . . as-yet-unrealized risks and contingencies" and fail to alert "the reader that some of these risks may already have come to fruition." *Berson v. Applied Signal Tech., Inc.*, 527 F.3d 982, 986 (9th Cir. 2008).

They analogize this case to *Flynn*, where a court in the Central District found that those plaintiffs had adequately pled that that the defendant's risk disclosures were misleading. 2016 WL 3360676, at *10–11. There, the defendant had allegedly warned that its "products may not be manufactured . . . in compliance with regulatory requirements, or its manufacturing facilities may not be able to maintain compliance with regulatory requirements." *Id.* at 11. But, before the defendant filed the documents containing the disclosure, a German regulatory agency had suspended the defendant's sole manufacturer's authorization to sell its goods in the European Union due to compliance issues. *Id.* at 2-3. The defendant's risk disclosure was deceptive because it knew that what it had warned was a mere possibility—its manufacturer's failure to comply with regulatory requirements—had already come to pass. *Id.* at 10-12.

But those facts are not analogous to the factual allegations before the Court. While Plaintiffs describe the risk disclosures as warning "that AMD's processors could be susceptible to security vulnerabilities," (opp'n at 7), this assertion is not accurate. Defendants' risk disclosures address the risks posed by "[d]ata breaches and cyber-attacks" and by "potential claims for damages resulting from loss of data from alleged vulnerabilities in the security of our processors" not the existence of a vulnerability. ACAC ¶¶ 52, 54, 56. Plaintiffs do not allege that AMD has

suffered any data breaches or cyber-attacks because of Spectre or that AMD has been subject to claims for damages resulting from a successful exploitation of Spectre. Nor do Plaintiffs allege that when Defendants filed the risk disclosures they had any contemporaneous reasons to believe that cyber-attacks, data breaches, or litigation because of Spectre were remotely likely. Unlike *Flynn*, the potential risks disclosed in the SEC filings had not come to fruition when Defendants filed the challenged risk disclosures.

The Third Circuit's decision *Williams v. Globus Medical, Inc.* is instructive. 869 F.3d 235 (3d Cir. 2017). There, the plaintiffs alleged that the defendant had made misleading omissions because it had already secretly decided to end its relationship with a distributors before filing a Form 10-K and a Form 10-Q that both warned, "if any of our independent distributors were to cease to do business with us, our sales could be adversely affected." *Id.* at 242. The Third Circuit reasoned that "[t]he risk actually warned of is the risk of adverse effects on sales—not simply the loss of independent distributors generally. Accordingly, the risk at issue only materialized—triggering Globus's duty to disclose—if sales were adversely affected at the time the risk disclosures were made." *Id.* Because those plaintiffs did not allege that the defendant's sales had suffered as a result of the decision to end the relationship with the distributor, the Third Circuit found that the defendant had no duty to disclose its decision to terminate its relationship with the distributor, and the risk disclosure was not misleading. *Id.* at 243. Here, the danger warned of by Defendants were cyber-attacks, data breaches, and resulting litigation—not the discovery of vulnerabilities in AMD's processors. The Court finds that Plaintiffs have not pled that AMD's risk disclosure statements were false or misleading.

2. The January Statements

Plaintiffs argue that the statements about Spectre that Defendants made in January 2018 were misleading. The statements on January 3 and 8, 2018 were false and misleading, they contend, because AMD knew from the Kocher article that Variant 2 was present on AMD's processors, but Defendants stated that that the risk of exploitation was "near zero" or "rare." *Id.* ¶¶ 6, 60, 63. Thus, those statements are prohibited "half-truths." *United States v. Laurienti*, 611 F.3d 530, 539 (9th Cir. 2010). The falsity of the January 3 and 8, 2018 statements is further

shown, Plaintiffs contend, by the January 11th statement that AMD's processors were susceptible to *both* variants of Spectre, and the accompanying drop in stock prices.

However, the Court finds that Plaintiffs have not adequately pled that the January 3 and 8, 2018 statements are false or misleading. Defendants represented that Variant 2 posed a "near zero" risk to AMD's processors, and that due to AMD's architecture, Variant 2 was "rare" and "difficult to access." ACAC ¶¶ 58, 59, 62. Plaintiffs' argument that these statements omitted that Variant 2 was present on their processors is simply not accurate. There is no conflict or omission between Defendants' statements that Variant 2 was "rare" and "difficult to access," and Plaintiffs' allegation that the Kocher article informed Defendants that researchers had observed Variant 2 on AMD's processors. *See id.* ¶¶ 60, 63. At most, Defendants represented on January 3, 2018 that "[v]ulnerability to Variant 2 has not been demonstrated on AMD processors to date," but Plaintiffs do not allege facts showing that Defendants knew that the Kocher Report researchers had observed Variant 2 on AMD's products when Defendants made that representation. Nor does AMD's later provision of patches and updates to protect against Variant 2 conflict AMD's assessment that Variant 2 posed a "near zero risk." Plaintiffs and their cited media report both misinterpret a "near zero risk" for "zero risk." *See id.* ¶¶ 60, 63, 67; Tom Warren, *AMD is releasing Spectre firmware updates to fix CPU vulnerabilities*, The Verge (Jan. 11, 2018), https://www.theverge.com/2018/1/11/16880922/amd-spectre-firmware-updates-ryzen-epyc. Plaintiffs do not allege that Variant 2 posed a greater than a "near-zero" risk to AMD's processors, that Variant 2 was more than "rare" on AMD's processors, or that Variant 2 is not "difficult to access."

To the extent the statements are misleading because they omit any reference to yet-to-be-announced patches or updates to protect against Variant 2, Plaintiffs' allegations are conclusory. ACAC ¶¶ 60, 63, 67. Plaintiffs plead no facts showing that Defendants had contemporaneous knowledge that patches and updates would be required when they made the statements. "[A] plaintiff seeking to plead falsity under the PSLRA generally must identify 'specific contemporaneous statements or conditions that demonstrate the intentional or the deliberately reckless false or misleading nature of the statements when made.'" *Rieckborn v. Jefferies LLC*, 81

F. Supp. 3d 902, 927 (N.D. Cal. 2015) (quoting *Ronconi v. Larkin*, 253 F.3d 423, 432 (9th Cir. 2001)); *see also Khoja*, 899 F.3d at 1008.

For much the same reasons, the Court finds that the January 11th statement is consistent with the other statements. The January 11th statement neither revealed new information nor contradicts the earlier statements. Plaintiffs argue that the earlier statements that AMD faced a "near zero risk of exploitation" is at odds with the statement that Variant 2 is "applicable to AMD processors," but this theory, like their theory on the risk disclosure statements, conflates a successful exploitation with a mere vulnerability. The information disclosed by Defendants on January 3 and 8, 2018 was "entirely consistent with the more detailed explanation" Defendants disclosed on January 11, 2018. *In re Yahoo! Inc. Sec. Litig.*, 611 F. App'x 387, 389 (9th Cir. 2015). Plaintiffs' allegation that on January 11, 2018, AMD's stock price dropped $0.12, or 0.99 percent does not support an inference that the market perceived AMD as changing it position on its susceptibility to Variant 2. One, the cases cited by Plaintiffs are off-point because they concerned drops of 31 percent and of about 26 percent. *See No. 84 Employer-Teamster Joint Council Pension Tr. Fund v. Am. W. Holding Corp.*, 320 F.3d 920, 935 (9th Cir. 2003); *In re Montage Technlogy Grp. Ltd. Sec. Litig.*, 2016 WL 1598666, at *7 (N.D. Cal. Apr. 21, 2016). And two, AMD's stock dropped by several time more on January 9, 2019—by $0.46—before Defendants allegedly revealed the alleged discrepancy. Ex. 2. The Court finds that Plaintiffs have not adequately pled that the January statements are false or misleading.

B. Scienter

Even if Plaintiffs had adequately pled that Defendants had made materially false or misleading statements or omissions, the Court would still find that they had not adequately pled scienter. "Scienter" refers to "a mental state embracing intent to deceive, manipulate, or defraud." *NVIDIA*, 768 F.3d at 1053 (quoting *Ernst & Ernst v. Hochfelder*, 425 U.S. 185, 193 n.12 (1976)). The Ninth Circuit has recognized that recklessness "may satisfy the element of scienter." *Id.* (quoting *Hollinger v. Titan Capital Corp.*, 914 F.2d 1564, 1568–69 (9th Cir.1990)). But, it must be "deliberate recklessness." *Id.* (quoting *In re Silicon Graphics Inc. Sec. Litig.*, 183 F.3d 970, 977 (9th Cir. 1999), as amended (Aug. 4, 1999)). "Deliberate recklessness means that the reckless

conduct reflects some degree of intentional or conscious misconduct." *Hatamian v. Advanced Micro Devices, Inc.*, 87 F. Supp. 3d 1149, 1161-62 (N.D. Cal. 2015) (citation omitted).

The PSLRA sets stringent standards for adequately pleading scienter. A complaint must "state with particularity facts giving rise to a strong inference that the defendant acted with the required state of mind." 15 U.S.C. § 78u-4(b)(2). In assessing whether a complaint fulfills this requirement, a court "must consider plausible, nonculpable explanations for the defendant's conduct, as well as inferences favoring the plaintiff. The inference that the defendant acted with scienter need not be irrefutable . . . or even the most plausible of competing inferences." *Tellabs*, 551 U.S. at 323-24 (quotations omitted). The Supreme Court has held that courts should consider "whether all of the facts alleged, taken collectively, give rise to a strong inference of scienter, not whether any individual allegation, scrutinized in isolation, meets that standard." *Id.* at 322-23. In the Ninth Circuit, courts apply this rule with a two-step process. First, courts should determine whether any allegation is, by itself, sufficient to support the strong inference of scienter. *NVIDIA*, 768 F.3d at 1056. If not, then courts should consider the allegations holistically. *Id.* A complaint will survive a motion to dismiss "only if a reasonable person would deem the inference of scienter cogent and at least as compelling as any opposing inference one could draw from the facts alleged." *Tellabs*, U.S. 551 at 324.

Plaintiffs raise three separate grounds allegedly showing scienter. But, none supports a strong inference of scienter on its own. First, Plaintiffs contend that because Project Zero notified AMD on June 1, 2017 that AMD's processors were susceptible to Variant 1, Defendants filed the risk disclosures and made the January 2018 statements with the knowledge that those representations were false or misleading. The Court finds that under these factual allegations, knowledge of AMD's susceptibility to Variant 1 is, on its own, not enough to plead a strong inference of scienter. Plaintiffs allege no facts showing that Defendants acted with either an intent to deceive, or with deliberate and reckless disregard for this knowledge in withholding disclosure until January 2018. Rather, Plaintiffs affirmatively plead a more compelling inference: that Defendants, in line with Project Zero's protocol, tried to prevent public disclosure of the vulnerabilities before updates and patches to fix the vulnerability were available. ACAC ¶¶ 38-40.

Second, Plaintiffs argue that they have sufficiently alleged facts to impute scienter to Su and Kumar under the core operations doctrine. Where, as here, "a complaint relies on allegations that management had an important role in the company but does not contain additional detailed allegations about the [management] defendants' actual exposure to [the allegedly concealed] information, it will usually fall short of the PSLRA standard" for alleging scienter. *S. Ferry LP, No. 2 v. Killinger*, 542 F.3d 776, 784 (9th Cir. 2008). Without considering other allegations, two exceptions to this rule exist. First, allegations about management's role in the company may "independently satisfy the PSLRA[']s scienter standard] where they are particular and suggest that defendants had actual access to the disputed information." *Id.* at 786. Or, second, the role of management can show scienter where "the nature of the relevant fact is of such prominence that it would be 'absurd' to suggest that management was without knowledge of the matter." *Id.* As to the first exception, the ACAC contains no allegations suggesting Su had access to or knowledge of Spectre prior to January 8, 2018, or that Kumar ever had any access to, or knowledge of Spectre. At most, Plaintiffs allege that Su and Kumar, pursuant to section 302 of the Sarbanes-Oxley Act, certified the SEC filings at issue. ACAC nn.19-21. But, "required certifications under Sarbanes–Oxley section 302(a), however, add nothing substantial to the scienter calculus." *Zucco Partners, LLC v. Digimarc Corp.*, 552 F.3d 981, 1003–04 (9th Cir. 2009), *as amended* (Feb. 10, 2009). *In re Cell Pathways, Inc.* is off-point. There, "the scienter allegations [did] not rest on [the individual defendants'] mere status within the company. Rather, Plaintiffs' allegations of the individual Defendants' knowledge [were] substantially more extensive," and included allegations about their access to undisclosed information, their responsibilities in company operations, their role in preparing the allegedly misleading statements, and their role in creating and running the drug trial at issue. 2000 WL 805221, at *7 (E.D. Pa. June 20, 2000). Plaintiffs make no similar allegations regarding Su or Kumar.

As to the second exception, while the ACAC contains allegations concerning the importance of the Ryzen processors to AMD's business and the theoretical harm of a successful exploitation of Spectre, it does not allege there was any reason for Defendants to believe such an

exploitation was at all likely. Thus, susceptibility of AMD's processors to Spectre was not so "prominen[t]" that it would be "absurd" for Su and Kumar not know about it. *Killinger*, 542 F.3d at 786. The cases cited by Plaintiffs all involved much more developed allegations about the prominence of the relevant issue. In *Berson*, the stop-work orders had "allegedly halted tens of millions of dollars of the company's work." 527 F.3d at 988. In *Mulligan v. Impax Laboratories, Inc.*, the allegations involved "substandard, non-compliant conditions pervading their company's manufacturing and quality control divisions—the heart of [the] company." 36 F. Supp. 3d 942, 970 (N.D. Cal. 2014). The district court found that "given the importance of manufacturing and quality control to the success of Impax and the fact that both areas of operation had been flagged by the FDA," the standard for scienter had been met. *Id.* And in *Reese v. Malone*, the Ninth Circuit found it "absurd" that management would not be aware of the compliance violations at issue "[i]n light of the magnitude of the violations, the immense public attention on BP in the wake of the spills, and the contemporaneous documents demonstrating management's awareness of the company's non-compliance with the Corrective Action Order. 747 F.3d 557, 579-80 (9th Cir. 2014), *overruled by City of Dearborn v. Align Tech., Inc.*, 856 F.3d 605 (9th Cir. 2017).

Finally, Plaintiffs argue that the eight days between AMD's announcement that the there was a "near zero risk" of exploitation through Spectre Variant 2 and the disclosure that its processors were susceptible to Spectre Variant 2 supports an inference of scienter. They contend that the inference the Court should draw is that Defendants knew that AMD's processors were susceptible on January 3, 2018, but withheld that information for eight days to strengthen their position against competitors, like Intel, that were more seriously affected by Spectre and/or Meltdown. They analogize the facts here to *Fecht v. Price Co.*, 70 F.3d 1078, 1082 (9th Cir. 1995), and *Roberti v. OSI Systems, Inc.*, 2015 WL 1985562 (C.D. Cal. Feb. 27, 2015). But, *Fecht* is a pre-PSLRA case, that follows a standard that "can no longer be said to constitute the sum of scienter pleading requirements." *Marksman Partners, L.P. v. Chantal Pharm. Corp.*, 927 F. Supp. 1297, 1309 (C.D. Cal. 1996); *Fecht*, 70 F.3d at 1082 n.4 ("With respect to scienter, the plaintiffs need simply say that scienter existed to satisfy the requirements of Rule 9(b)." (quotation and

alteration omitted)). And in *Roberti*, the Court explicitly found that none of the allegations independently established scienter. 2015 WL 1985562, at *11. The Court finds that Plaintiffs' proposed inference lacks support from the ACAC. To begin, Plaintiffs do not allege that Defendants knew AMD's processors were susceptible to Variant 2 prior to January 3, 2018—the day the Kocher article was published. ACAC ¶¶ 41, 46, n.11. As they concede, the report Project Zero provided to AMD in June 2017 did not say that Variant 2 had been observed on AMD's processors. *Id.* ¶ 45. Second, while the ACAC does allege that Spectre and Meltdown affected Intel (ACAC ¶¶ 41, 44), it does not allege that Intel was "more seriously affected" than AMD. Opp'n at 20. Nor does the ACAC allege how Intel's stock—or any other competitor's stock—responded to the disclosure of Spectre and Meltdown making any such comparative inference impossible to draw from this complaint. Plaintiffs also do not allege facts illustrating why Defendants would have believed that an eight-day delay would benefit AMD more than immediately disclosing its alleged susceptibility to Variant 2. In short, Plaintiffs have failed to "state with particularity facts giving rise to a strong inference" of scienter based solely on the eight days in between the statements. 15 U.S.C. § 78u-4(b)(2).

Having determined that none of Plaintiffs allegations independently support a sufficient inference of scienter, the Court now considers Plaintiffs allegations holistically. *Zucco*, 552 F.3d at 992. Plaintiffs contend that their allegations support an inference that after Defendants learned of their processors' susceptibility to Spectre Variant 1 on June 1, 2017, they omitted any reference to the vulnerability in their SEC filings from the class period. Then, after Project Zero disclosed both Spectre Variants and Meltdown on January 3, 2018, Defendants concealed their processors' susceptibility to Variant 2 in order to gain a benefit over Intel and their other competitors. Defendants argue that the correct inference to draw from the ACAC is that when AMD learned of Spectre, it followed Project Zero's protocol by first working to research the vulnerability and then develop any necessary mitigations. Only then did AMD publicly discuss the vulnerability. Thus, Defendants argue, there is no strong inference of scienter.

Based on the facts alleged in the ACAC, the Court finds Defendants' proposed inference to

be substantially more compelling than the one advanced by Plaintiffs. As discussed above, Plaintiffs do not allege sufficient facts to support any inference that that the January statements were intended to provide AMD with a boost over its competitors. Moreover, as opposed to acting with reckless disregard for Project Zero's June 1, 2017 report in issuing the challenged risk disclosures, the more compelling inference is that Defendants were acting in compliance with Project Zero's protocol by first investigating the vulnerability and developing a fix before disclosing the vulnerability. This case is analogous to *NVIDIA*. There, the defendant company did not disclose flaws in its processors for about a year. 768 F.3d at 1050-51. When it finally did, its stock price fell 31 percent and it took a $150-200 million charge to cover costs arising from the defects. *Id.* The plaintiffs there alleged that NVIDIA had acted with scienter because it had delayed the disclosure until it had readied replacement chips. *Id.* at 1060. The Ninth Circuit disagreed. It found that "a more compelling inference is that NVIDIA did not disclose because it was investigating the extent of the problem, whether it was responsible for it, and if so, whether it would exhaust the reserve [of money to cover product defects]." *Id.* at 1065. Plaintiffs make no attempt to distinguish the case at hand from *NVIDIA*.

Accordingly, the Court finds that the ACAC fails to plead scienter under the PSLRA's heightened standards.

IV. Section 20(a) of the Exchange Act

In order to maintain claims under Section 20(a), a plaintiffs must "adequately plead a primary violation of section 10(b)." *Zucco*, 552 F.3d 990. If the plaintiff does not meet that pleading requirement, then the "Section 20(a) claims may be dismissed summarily." *Id.* The therefore Court dismisses Plaintiffs claims under Section 20(a).

V. Conclusion

For the reasons discussed above, the Court grants Defendants' motion to dismiss. Plaintiffs may file an amended complaint within 21 days of this order.

IT IS SO ORDERED.

Dated: May 23, 2019

EDWARD J. DAVILA
United States District Judge

United States District Court
Northern District of California