MATTHEW W. CLOSE (S.B. #188570)
mclose@omm.com
BRITTANY ROGERS (S.B. #274432)
brogers@omm.com
O'MELVENY & MYERS LLP
400 S. Hope Street
Los Angeles, CA 90071-2899
Telephone: (213) 430-6000
Facsimile: (213) 430-6407

Attorneys for Defendants
Advanced Micro Devices, Inc.,
Lisa T. Su, and Devinder Kumar

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

DOYUN KIM, individually and on behalf of all others similarly situated,

Plaintiff,

v.

ADVANCED MICRO DEVICES, INC., a Delaware corporation, LISA T. SU, and DEVINDER KUMAR,

Defendants.

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

DEFENDANTS ADVANCED MICRO DEVICES, INC., LISA T. SU, AND DEVINDER KUMAR'S NOTICE OF MOTION AND MOTION TO DISMISS CONSOLIDATED AMENDED COMPLAINT PURSUANT TO FED. R. CIV. P. 12(B)(6) AND 9(B), AND THE PRIVATE SECURITIES LITIGATION REFORM ACT; MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT THEREOF

[Request for Judicial Notice and Declaration of Matthew W. Close Filed Concurrently]

Date: January 17, 2019
Time: 9:00 a.m.
Place: Courtroom 4, 5th Floor
Judge: Hon. Edward J. Davila

TABLE OF CONTENTS

Page

NOTICE OF MOTION AND ISSUES TO BE DECIDED 1

MEMORANDUM OF POINTS AND AUTHORITIES 2

I. INTRODUCTION AND SUMMARY OF ARGUMENT 2

II. FACTUAL ALLEGATIONS 5

III. ARGUMENT 9

A. The CAC Fails to Allege a Materially False or Misleading Statement 11

1. AMD's SEC Filings Disclosed Risks Associated with Potential Security Vulnerabilities and Were Not Materially False or Misleading 11

2. AMD's Press Release on Ryzen Products Was Not Materially False or Misleading 15

3. AMD's January 2018 Statements About Spectre Were Not Materially False or Misleading 18

4. Plaintiffs' Allegations and Judicially Noticeable Facts Demonstrate That Spectre Was Not Material to Investors 20

B. Plaintiffs Fail to Plead Any Inference of Scienter 21

C. The CAC Fails to State a Section 20 Claim Against Dr. Su and Mr. Kumar 25

IV. CONCLUSION 25

TABLE OF AUTHORITIES

Page(s)

CASES

Brodsky v. Yahoo! Inc.,
630 F. Supp. 2d 1104 (N.D. Cal. 2009) 5, 23

Brody v. Transitional Hosps. Corp.,
280 F.3d 997 (9th Cir. 2002) 4, 11, 16, 24

Brown v. China Integrated Energy, Inc.,
875 F. Supp. 2d 1096 (C.D. Cal. 2012) 22

Bruce v. Suntech Power Holdings Co.,
2013 WL 6843610 (N.D. Cal. Dec. 26, 2013) 25

City of Roseville Emps.' Ret. Sys. v. Sterling Fin. Corp.,
963 F. Supp. 2d 1092 (E.D. Wash. 2013) 13

Colyer v. Acelrx Pharm., Inc.,
2015 WL 7566809 (N.D. Cal. Nov. 25, 2015) 24

Dura Pharm., Inc. v. Broudo,
544 U.S. 336 (2005) 9

Ernst & Ernst v. Hochfelder,
425 U.S. 185 (1976) 10, 24

Ganino v. Citizens Utils. Co.,
228 F.3d 154 (2d Cir. 2000) 14

Garfield v. NDC Health Corp.,
466 F.3d 1255 (11th Cir. 2006) 24

Glazer Capital Mgmt., LP v. Magistri,
549 F.3d 736 (9th Cir. 2008) 24

In re AstraZeneca Sec. Litig.,
559 F. Supp. 2d 453 (S.D.N.Y. 2008) 23

In re Convergent Tech. Sec. Litig.,
948 F.2d 507 (9th Cir. 1991) 19

In re Daou Sys., Inc.,
411 F.3d 1006 (9th Cir. 2005) 10

In re Downey Sec. Litig.,
2009 WL 736802 (C.D. Cal. Mar. 18, 2009) 25

In re Dynavax Sec. Litig.,
2018 WL 2554472 (N.D. Cal. June 4, 2018) 13

TABLE OF AUTHORITIES
(continued)

Page(s)

In re GlenFed, Inc. Sec. Litig.,
42 F.3d 1541 (9th Cir. 1994) 10, 16, 18

In re Hansen Nat. Corp. Sec. Litig.,
527 F. Supp. 2d 1142 (C.D. Cal. 2007) 21, 24

In re Intuitive Surgical Sec. Litig.,
65 F. Supp. 3d 821 (N.D. Cal. 2014) 12, 14, 19

In re NVIDIA Corp. Sec. Litig.,
768 F.3d 1046 (9th Cir. 2014) 5, 14, 22

In re Read-Rite Corp.,
335 F.3d 843 (9th Cir. 2003) 19

In re Rigel Pharm., Inc. Sec. Litig.,
697 F.3d 869 (9th Cir. 2012) 10

In re Splash Tech. Holdings, Inc. Sec. Litig.,
160 F. Supp. 2d 1059 (N.D. Cal. 2001) 15

In re U.S. Aggregates, Inc. Sec. Litig.,
235 F. Supp. 2d 1063 (N.D. Cal. 2002) 23–24

In re VeriFone Sec. Litig.,
2014 WL 3920322 (N.D. Cal. Aug. 8, 2014) 17

In re Verity, Inc. Sec. Litig.,
2000 WL 1175580 (N.D. Cal. Aug. 11, 2000) 4, 12

In re Yahoo! Inc. Sec. Litig.,
611 F. App'x 387 (9th Cir. 2015) 19

Janus Capital Grp., Inc. v. First Derivative Traders,
564 U.S. 135 (2011) 17

Kelly v. Elec. Arts, Inc.,
2015 WL 1967233 (N.D. Cal. Apr. 30, 2015) 15

Lapiner v. Camtek, Ltd.,
2011 WL 445849 (N.D. Cal. Feb. 2, 2011) 24

LifeLock, Inc. Sec. Litig.,
690 F. App'x 947 (9th Cir. 2017) 16

Mallen v. Alphatec Holdings, Inc.,
2013 WL 1294640 (S.D. Cal. Mar. 28, 2013) 11, 20

TABLE OF AUTHORITIES
(continued)

Page(s)

Mallen v. Alphatec Holdings, Inc.,
861 F. Supp. 2d 1111 (S.D. Cal. 2012) 10

Manulife Fin. Corp. Sec. Litig.,
276 F.R.D. 87 (S.D.N.Y. 2011) 12

Marx v. Comput. Scis. Corp.,
507 F.2d 485 (9th Cir. 1974) 21

Metzler Inv. GMBH v. Corinthian Colls., Inc.,
540 F.3d 1049 (9th Cir. 2008) 10, 17

Mohebbi v. Khazen,
50 F. Supp. 3d 1234 (2014) 22

Ong v. Chipotle Mexican Grill, Inc.,
294 F. Supp. 3d 199 (S.D.N.Y. 2018) 13

Or. Pub. Emps. Ret. Fund v. Apollo Grp. Inc.,
774 F.3d 598 (9th Cir. 2014) 23

Plumbers & Steamfitters Local 773 Pension Fund v. Canadian Imperial Bank of Commerce,
694 F. Supp. 2d 287 (S.D.N.Y. 2010) 23

Retail Wholesale & Dep't Store Union Local 338 Ret. Fund v. Hewlett-Packard Co.,
845 F.3d 1268 (9th Cir. 2017) 20

Ronconi v. Larkin,
253 F.3d 423 (9th Cir. 2001) 11

SEC v. Aline Sec. Corp.,
308 F. Supp. 3d 775 (S.D.N.Y. 2018) 14

SEC v. Reyes,
491 F. Supp. 2d 906 (N.D. Cal. 2007) 21

Shemian v. Research In Motion Ltd.,
2013 WL 1285779 (S.D.N.Y. Mar. 29, 2013) 15

Swartz v. KPMG LLP,
476 F.3d 756 (9th Cir. 2007) 17

Tellabs, Inc. v. Makor Issues & Rights, Ltd.,
551 U.S. 308 (2007) 10, 21, 22

TABLE OF AUTHORITIES
(continued)

Page(s)

TSC Indus., Inc. v. Northway, Inc.,
426 U.S. 438 (1976) 20, 21

Zucco Partners, LLC v. Digimarc Corp.,
552 F.3d 981 (9th Cir. 2009) 5, 10, 24, 25

STATUTES

15 U.S.C. § 78t(a) 25

15 U.S.C. § 78u–4(b)(1)(B) 10

15 U.S.C. § 78u–4(b)(2)(A) 10

15 U.S.C. § 78u–4(b)(3)(A) 10

OTHER AUTHORITIES

Securities and Exchange Commission, Division of Corporation Finance, *CF Disclosure Guidance: Topic No. 2, Cybersecurity*, October 13, 2011 ..... 14, 25

International Organization for Standardization and International Electrotechnical Commission, *Information technology — Security techniques — Vulnerability disclosure*, February 15, 2014 ..... *passim*

REGULATIONS

17 C.F.R. § 240.10b–5 9

NOTICE OF MOTION AND MOTION TO DISMISS

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:

PLEASE TAKE NOTICE that on January 17, 2019, at 9:00 a.m., or as soon thereafter as this matter may be heard in Courtroom 4, 5th floor, of the above-captioned Court, located at 280 South 1st Street, San Jose, CA 95113, Defendants Advanced Micro Devices, Inc. ("AMD"), Lisa T. Su, and Devinder Kumar (the "Individual Defendants," collectively with AMD, "Defendants") will, and hereby do, move the Court for an order dismissing the Consolidated Amended Complaint ("CAC") with prejudice, pursuant to Federal Rules of Civil Procedure 12(b)(6) and 9(b), as well as the Private Securities Litigation Reform Act of 1995, 15 U.S.C. § 78u-4 et seq. (2010) ("PSLRA").

This Motion is based on this Notice of Motion and Motion, the accompanying Memorandum of Points and Authorities, the Request for Judicial Notice, the Declaration of Matthew W. Close and exhibits attached thereto, the arguments of counsel, all pleadings and papers on file in this action, and such other further written and oral argument as may be presented to the Court at the hearing on this Motion or before the Court's decision.

ISSUES TO BE DECIDED

1. Whether Plaintiffs' claim under Section 10(b) of the Securities Exchange Act of 1934 ("Section 10(b)") should be dismissed because the CAC fails to allege adequately that any Defendant made a materially false or misleading statement.

2. Whether Plaintiffs' claim under Section 10(b) should be dismissed because the CAC fails to allege facts giving rise to a strong inference that any Defendant acted with scienter.

3. Whether Plaintiffs' claim under Section 20(a) of the Securities Exchange Act of 1934 ("Section 20") should be dismissed because the CAC fails to allege an underlying Section 10(b) claim or the facts establishing that either Individual Defendant is a control person for secondary liability purposes.

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION AND SUMMARY OF ARGUMENT

In a digitally interconnected world, cybersecurity risks are ubiquitous. Hackers and other malicious actors work around the clock to trick computer users into exposing data to phishing attempts and fraudulent websites. Cybercriminals also seek to identify and develop attacks to exploit hardware and software to the detriment of end users. For technology companies like AMD, thwarting the malicious plans of these bad actors requires not just vigilance but prudence.

When presented with a possible vulnerability, companies understand that prior to publicly announcing it they must first assess the suspected threat for viability—to determine whether and to what extent a theoretical vulnerability can actually be exploited in the real world. The timing of public announcement is important since alerting bad actors to the existence of a potential vulnerability that may be viable and may have real-world consequences before a mitigation is in place only invites greater risk of attack. To minimize the danger of prematurely publicizing potential vulnerabilities and inadvertently encouraging opportunistic exploitation, the technology industry has developed a protocol known as "responsible disclosure." (*See* Ex. 1.)[1] When a potential vulnerability is discovered, possibly affected companies are given time to evaluate it and develop workarounds or other mitigations, if necessary, before any announcement is made. (*Id.*) Responsible disclosure is not securities fraud. Rather, it protects end users of complex and evolving technologies, and it deters those who seek to harm them.

In June 2017, Google Project Zero ("GPZ") informed AMD and its competitors at Intel and ARM Holdings that their processors might be vulnerable to attacks that could expose end users' data to malicious actors. (*See* CAC ¶¶ 4, 47.) Although there was no basis to believe this potential vulnerability had been practiced in the real world, once alerted, AMD worked to assess whether there was any real-world threat. Where appropriate, AMD also worked to develop defenses before GPZ announced the potential vulnerability, which was later dubbed "Spectre" by another set of researchers. (*See id.* ¶ 58.) GPZ released details about Spectre in January 2018

[1] Citations to "Ex. __" are to the exhibits to the Declaration of Matthew W. Close in support of Defendants' Request for Judicial Notice.

after leaks began. (*See id.* ¶¶ 6, 41.) During the following week, AMD made several public statements, consistently explaining that Spectre remained theoretical—that it "has not been seen in the public domain"—but nonetheless identifying potential risks and planned mitigations for Spectre's variations. (*Id.* ¶¶ 58, 62, 66.)[2]

Although there was significant press coverage when GPZ announced Spectre, AMD's stock price hardly moved. (*See* Ex. 2.) Investors were well aware of the possibility that malicious actors might try to manipulate computer processors in an attempt to improperly access end-user data. AMD ensured that investors knew. Specifically, throughout the class period, AMD disclosed to investors that: (1) "Data breaches and cyber-attacks could compromise [AMD's] intellectual property or other sensitive information, be costly to remediate and cause significant damage to [AMD's] business and reputation"; (2) "Cyber-attacks . . . could also cause [AMD] to incur significant remediation costs, result in product development delays, disrupt key business operations and divert attention of management and key information technology resources"; and (3) AMD "could be subject to potential claims for damages resulting from loss of data from alleged vulnerabilities in the security of [AMD's] processors." (*Id.* ¶¶ 52, 54, 56; *see also id.* ¶ 31.)

Fortunately, Spectre has not resulted in these or any other material consequences, and Plaintiffs do not allege otherwise. Plaintiffs do not allege that Spectre has ever actually been exploited in the "public domain" to gain access to end-user data. (*Cf. id.* ¶ 58.) And Plaintiffs do not allege that AMD has restated its financial statements, taken a charge to its earnings, altered its loss contingency reserves, or suffered any materially adverse business consequences due to Spectre. AMD's stock price dropped just 12 cents—less than 1%—on January 11, 2018, the day Plaintiffs claim the "truth" was revealed. (*See* Ex. 2.) In the weeks that followed, AMD's stock price increased by more than a dollar. On August 3, 2018, the day that Plaintiffs filed their CAC, AMD's stock price closed at $18.49, up more than 50% from the final day of the class period.[3]

---

[2] AMD also explained that a second potential threat, "Meltdown," does not apply to AMD because of its processors' "architecture differences," (*id.* ¶ 58), and Plaintiffs do not allege that AMD's processors are even theoretically susceptible to Meltdown.

[3] *See also* Brian Sozzi, *AMD Is One of the Hottest Stocks on the Planet*, THE STREET (Aug. 27,

Despite the significant gains shareholders realized, Plaintiffs allege that AMD along with the Individual Defendants somehow violated federal securities laws between GPZ's initial report of potential security threats and AMD's public statement on January 11. Plaintiffs are wrong. Public companies have no duty to disclose all information in their possession. *See In re Verity, Inc. Sec. Litig.*, 2000 WL 1175580, at *4 (N.D. Cal. Aug. 11, 2000) ("[A] duty to disclose 'does not arise from the mere possession of nonpublic market information.'"). Instead, Section 10(b) liability requires a materially false or misleading statement, and Plaintiffs fail to identify a single one, either before or after Spectre was announced.

At most, Plaintiffs' claims can be construed as asserting that AMD and the Individual Defendants should have released more detailed information about Spectre before January 11. But precipitous disclosures without first understanding the nature of the potential threat and developing a mitigation, if warranted, could have been dangerous—putting in jeopardy the data of end users by alerting bad actors to the existence of a potential vulnerability before understanding its applicability. (*See* CAC ¶ 38 (citing GPZ policy of not reporting vulnerabilities until "a patch is available").) And nowhere in the CAC do Plaintiffs explain how any challenged statements created an impression that differed from reality. *See Brody v. Transitional Hosps. Corp.*, 280 F.3d 997, 1006 (9th Cir. 2002) ("To be actionable under the securities laws, an omission must be misleading; in other words it must affirmatively create an impression of a state of affairs that differs in a material way from the one that actually exists."). Plaintiffs do not explain what details about Spectre—if any—Defendants should have included in the challenged statements, how those technical and still-developing details would have altered the total mix of information available to investors (who are well aware of the dangers of cybersecurity threats and dedicated bad actors), or how excluding further details rendered any challenged statements misleading. There are simply no factual allegations to establish that AMD's business faced unique and material risks from Spectre such that AMD could not conclude in its reasonable judgment that the prudent

---

2018), https://www.thestreet.com/technology/amd-is-one-of-the-hottest-stocks-on-the-planet-14694050 ("Shares of the chip-maker have skyrocketed 24% in August . . . . AMD's stock has surged about 120% this year . . . ."). (Ex. 3.)

course was to follow the industry's established "responsible disclosure" protocols. And time has proven that judgment to be entirely accurate.

Plaintiffs also fail to make any case, let alone a cogent or compelling one, for scienter. Their CAC does not even try. (*See* CAC ¶¶ 83–84.) As the Ninth Circuit has made clear, scienter cannot be shown by simply alleging that a company took necessary time to evaluate a potential vulnerability, assessed its root cause, and disclosed the specific details of the issue once a mitigation was in place. *In re NVIDIA Corp. Sec. Litig.*, 768 F.3d 1046, 1056 (9th Cir. 2014) ("Any inference of scienter requires more than this."). And the CAC does not allege any motive suggestive of ill intent. While it contains fleeting references to management positions and the Individual Defendants' signatures on public filings, courts routinely reject such allegations as insufficient to plead a strong inference of scienter. *See, e.g.*, *Zucco Partners, LLC v. Digimarc Corp.*, 552 F.3d 981, 1003–04 (9th Cir. 2009) (signing public filings, alone, is insufficient to establish scienter); *Brodsky v. Yahoo! Inc.*, 630 F. Supp. 2d 1104, 1118 (N.D. Cal. 2009) (rejecting allegations that defendants must have known about misrepresentations due to executive positions).

Finally, because Plaintiffs' Section 10(b) claim fails, their Section 20 claim for control-person liability fails as a matter of law. The CAC also fails to state a Section 20 claim because it does not allege with the requisite specificity that any Individual Defendant exercised actual power or control over the challenged statements. These fundamental deficiencies riddling the CAC require dismissal.

II. FACTUAL ALLEGATIONS

AMD is a multinational semiconductor company that designs and has manufactured microprocessors that are offered as standalone devices or incorporated into accelerated processing units. (*See generally* Ex. 4.) According to Plaintiffs, AMD's products are offered in "retail and commercial markets for desktop, notebook, mobile, and server processors." (CAC ¶ 3.)

Finding and Fixing Potential Security Vulnerabilities. AMD is "vigilant" in identifying and mitigating potential "security vulnerabilities" in its products. (*Id.* ¶ 36.) Likewise, other technology companies take a proactive approach to make computing safer for end users; Google,

for example, formed GPZ in 2014 to research and test potential security vulnerabilities to "mak[e] the internet safer." (*Id.* ¶ 37.) GPZ's stated objectives are to ensure "users [are] able to use the web without fear that a criminal or state-sponsored actor is exploiting software bugs to infect [their] computer[s]" and to stop cyberattacks, "reducing the number of persons that such targeted attacks harm[]." (*Id.*) While its goals include "transparency and a cooperative relationship" with technology companies, GPZ's so-called "bug reports" typically go public only "once a patch is available." (*Id.* ¶ 38.) This approach is consistent with the industry practice of responsible disclosure.

So high are the stakes of prematurely disclosing security vulnerabilities that the International Organization for Standardization ("ISO") and the International Electrotechnical Commission ("IEC")—two organizations that "form the specialized system for worldwide standardization"—issued an international standard in 2014 for identifying, mitigating, and disclosing potential vulnerabilities ("ISO Protocol"). (Ex. 1.) The ISO Protocol makes clear that when a "finder" like GPZ notifies a company about a potential security vulnerability, the company should first investigate the report and, if verified, develop and deploy effective mitigation techniques before informing users of the potential vulnerability. (*Id.* at 8.) As long as the potential vulnerability "is not actively exploited by attackers, it is desirable to issue the advisory and the resolution promptly ***after*** it becomes available." (Ex. 1 (emphasis added).) This is because "vulnerability information may be used to attack vulnerable products." (*Id.* at 9; *see also id.* at 1 ("Inappropriate disclosure of a vulnerability could not only delay the deployment of the vulnerability resolution but also give attackers hints to exploit it.").)

AMD's Risk Disclosures of Potential Security Vulnerabilities. Even before AMD began "to address [GPZ's] findings," (CAC ¶ 58), it publicly disclosed risks stemming from potential security vulnerabilities in its processors. In its May 8, 2017 Form 10-Q, for example, AMD cautioned that it "could be subject to potential claims for damages resulting from loss of data from alleged vulnerabilities in the security of our processors." (*Id.* ¶ 52.) The same language appeared in each of its subsequent Form 10-Qs throughout the class period. (*Id.* ¶¶ 54, 56.)

AMD also repeatedly made clear that its processors, like any computer processor, could

be targeted by bad actors seeking to hurt end users. Throughout the class period, AMD disclosed on its website that with the expansion of new technologies and products "comes a corresponding increase in security vulnerabilities and risks to sensitive data as it is being transported or stored." (Exs. 5 and 6.) AMD acknowledged "evolving data security threats" and "the evolution of security risks in cyberspace," as well as the need for "security solutions." (*Id.*) It also disclosed its efforts to develop such solutions, including by engaging in "technology research and development . . . to promote strong IT security protection." (*Id.*)

As part of these efforts to impede bad actors, AMD has highlighted various security features in its products. On June 29, 2017, for example, AMD noted that its Ryzen products offered "transparent secure memory encryption," "secure boot process," and "independent DRAM encryption" as features intended to mitigate potential security threats. (CAC ¶ 49.)[4] Nowhere did AMD describe its products as impervious to external threats; rather, the company expressly incorporated risk disclosures in its SEC filings and press releases, specifically warning investors of the possibility that third parties could seek to exploit "alleged vulnerabilities in the security of [its] processors." (Ex. 7; *see also* CAC ¶ 52.)

Spectre and Alleged Vulnerabilities to Speculative Side-Channel Attacks. In 2017, GPZ discovered a potential security vulnerability in virtually all modern computer processers allegedly related to a processing feature called speculative execution—an industry standard for decades. (CAC ¶ 47.) Speculative execution, along with "branch prediction," increases processing speeds by identifying the most probable set of commands that a particular end user will wish to make and provisionally executing the program on the predicted path. (*Id.* ¶¶ 42–43.) This allows the processor to move along the path more quickly because it anticipates and starts to execute possible commands before they are entered. (*Id.*) By enhancing performance, speculative execution and branch prediction also enhance consumers' experiences. (*See id.* ¶¶ 4, 41.)

The particular threat that allegedly impacts AMD's processors has a few different

[4] Plaintiffs cite a third-party website that has allegedly reposted AMD's June 29, 2017 "press release and accompanying presentation." (CAC ¶ 48; *id.* n.17.) The press release also appears on AMD's website, where it expressly incorporates AMD's most recent Form 10-Q disclosing various risks, including security vulnerabilities in its processors. (*See* Ex. 7.)

variations, which collectively have been called Spectre. (*See id.* ¶ 41.) As told by Plaintiffs, the theory behind Spectre is that a malevolent actor could hypothetically write and apply code that causes a processor to mispredict an execution path and speculatively execute instructions that it otherwise would not execute. (*Id.* ¶ 42.) According to reports cited in the CAC, attackers could seek to obtain and potentially exploit information theoretically revealed on the mispredicted path by gaining access to a processor's functions via indirect "side channels"—what is known as a speculative side-channel attack. (*See id.*) In other words, Plaintiffs allege that an attacker could hypothetically "gain access to secure information" such as "passwords and credit card information," (*id.* ¶ 43), even though they do not allege that Spectre has surfaced "in the public domain." (*Id.* ¶ 58.)

Following its normal processes and responsible disclosure principles, Plaintiffs allege that GPZ alerted AMD and other hardware and software companies about the potential for speculative side-channel attacks on June 1, 2017. (*Id.* ¶ 47.) As set forth in the CAC, GPZ's standard protocol is to give companies time to evaluate and address potential threats before going public—usually enough time for a mitigation to become available, if needed. (*Id.* ¶¶ 38–39.)

Potential for Speculative Side-Channel Attacks Made Public. On January 3, 2018, after a series of leaks, GPZ publicly reported the potential for speculative side-channel attacks. (*Id.* ¶¶ 41, 58.) On the same day, AMD made a public statement explaining that after learning about a potential threat from GPZ, AMD immediately began addressing GPZ's findings. (*Id.* ¶ 58.) AMD acknowledged that two variants of Spectre were potentially applicable to its processors. (*Id.*) Software and operating system updates would be made available to mitigate the risks of Variant 1, with "[n]egligible performance impact expected." (*Id.*) But AMD believed that their processors' unique architecture meant that there was a "near zero risk of exploitation" under Variant 2. (*Id.*) An AMD spokesperson allegedly reiterated that there was a "near zero risk" of a bad actor exploiting Variant 2 on an AMD processor. (*Id.* ¶ 59.) The CAC does not allege that there were or have since been any successful exploitations of Variant 2 on an AMD processor.

On January 8, 2018, during a CNBC interview, AMD's Chief Executive Officer, Dr. Su, echoed these statements: AMD was actively working to develop mitigations for Variant 1, and

exploitation of Variant 2, though possible, would be "rare" and "difficult to access." (*Id.* ¶ 62.) Likewise, on January 11, 2018, AMD again distinguished between the potential applicability of Variants 1 and 2. (*Id.* ¶ 65.) As to Variant 1, AMD said it "is applicable to AMD processors" and could be "contained with an operating system (OS) patch." (*Id.*) While acknowledging that its processors could be susceptible to Variant 2 in theory, the company reiterated that "AMD's processor architectures make it difficult to exploit Variant 2." (*Id.*)

AMD's Stock Price Soars. On the day that news of Spectre—and AMD's planned mitigation efforts—became public, AMD's stock rose $0.57, from a close on January 2 of $10.98 to a close on January 3 of $11.55. (*Id.* ¶¶ 58– 61.) After the January 11 statement, when AMD again acknowledged potential susceptibility to Spectre Variants 1 and 2, (*id.* ¶ 66), the stock price dipped a mere $0.12 to a close of $12.02 on January 12. (*Id.* ¶ 68); (*see also* Ex. 2.) AMD's stock price skyrocketed over the following months. On August 3, 2018, the day Plaintiffs filed their CAC, AMD's stock price closed at $18.49. (*See* Ex. 2.)

Plaintiffs' CAC. In the CAC, Plaintiffs allege that Defendants made false or misleading statements in SEC filings and public announcements between May 8, 2017, and January 8, 2018. (CAC ¶¶ 51–52, 54, 56, 58–59, 62.) They also allege that statements about AMD products' security features were false and misleading because of Defendants' supposed knowledge of Spectre. (*Id.* ¶¶ 48–50.) Claiming violations of Section 10(b) and Section 20, (*id.* ¶¶ 79–94), Plaintiffs hope to represent a nationwide class of "all those who purchased or otherwise acquired AMD common shares traded on the NASDAQ during the Class Period[.]" (*Id.* ¶ 70.) For the reasons stated in this Motion, the CAC fails to state a claim under the federal securities laws.

III. ARGUMENT

To avoid dismissal, Plaintiffs must satisfy an intentionally high pleading standard. A claim for a violation of Section 10(b) and Rule 10b–5 thereunder (17 C.F.R. § 240.10b–5), requires a plaintiff to allege (1) a material misrepresentation or omission, (2) scienter, (3) a connection with the purchase or sale of a security, (4) reliance, (5) economic loss, and (6) loss causation. *Dura Pharm., Inc. v. Broudo*, 544 U.S. 336, 341–42 (2005). Section 10(b) claims are subject to Federal Rule of Civil Procedure 9(b)'s particularity requirements, as well as the

PSLRA's more "[e]xacting pleading requirements." *Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 313 (2007). To plead fraud with particularity under Rule 9(b), a "plaintiff must set forth what is false or misleading about a statement, and why it is false." *In re GlenFed, Inc. Sec. Litig.*, 42 F.3d 1541, 1548 (9th Cir. 1994) (*en banc*), *superseded on other grounds as stated in SEC v. Todd*, 642 F.3d 1207, 1216 (9th Cir. 2011). Conclusory statements unsupported by specific facts are insufficient. *See Mallen v. Alphatec Holdings, Inc.*, 861 F. Supp. 2d 1111, 1127–30 (S.D. Cal. 2012) ("*Mallen I*").

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). It requires that a plaintiff "specify each statement alleged to have been misleading, the reason or reasons why the statement is misleading, and, if an allegation regarding the statement or omission is made on information and belief . . . all facts on which that belief is formed." 15 U.S.C. § 78u–4(b)(1)(B). If the complaint does not satisfy these requirements, "the court shall, on the motion of any defendant, dismiss the complaint." *Id*. § 78u–4(b)(3)(A); *see also Metzler Inv. GMBH v. Corinthian Colls., Inc*., 540 F.3d 1049, 1072 (9th Cir. 2008).

To allege scienter, a plaintiff must state with particularity facts giving rise to a strong inference that the defendant acted intentionally, or with deliberate recklessness, to disseminate false or misleading information. 15 U.S.C. § 78u–4(b)(2)(A); *In re Daou Sys., Inc.*, 411 F.3d 1006, 1014–15 (9th Cir. 2005). Scienter is "a mental state embracing intent to deceive, manipulate, or defraud." *Ernst & Ernst v. Hochfelder*, 425 U.S. 185, 193 n.12 (1976). Courts apply a dual inquiry in deciding whether scienter allegations satisfy the PSLRA's stringent pleading standards. First, courts consider whether any of the allegations, standing alone, is sufficient to create a strong inference of scienter. *Zucco*, 552 F.3d at 992. If none is sufficient, courts apply the same analysis to the allegations taken as a whole. *Id*. In all cases, however, courts "must take into account plausible opposing inferences" from the allegations and judicially noticed facts. *Tellabs*, 551 U.S. at 323. A plaintiff's scienter allegations are adequate 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." *Id.* at 324. "Where pleadings are not sufficiently particularized or where, taken as a whole, they do not raise a 'strong inference' that misleading statements were knowingly or [with] deliberate recklessness made to investors, a private securit[i]es complaint is properly dismissed under Rule 12(b)(6)." *Mallen v. Alphatec Holdings, Inc.* ("*Mallen II*"), 2013 WL 1294640, at *9 (S.D. Cal. Mar. 28, 2013) (citing *Ronconi v. Larkin*, 253 F.3d 423, 429 (9th Cir. 2001)). Because Plaintiffs cannot satisfy any of these requirements, the Court should dismiss the CAC.

A. The CAC Fails to Allege a Materially False or Misleading Statement

Plaintiffs challenge three categories of statements but fail to allege facts to establish how or why any were materially false or misleading. The first set of statements are risk disclosures in a series of SEC filings during the class period, in which AMD warned investors that it "could be subject to potential claims for damages resulting from loss of data from alleged vulnerabilities in the security of its processors." (CAC ¶¶ 51–52, 54, 56.) The second is a June 29, 2017 press release and accompanying presentation in which AMD discussed its Ryzen products and advertised their various security features. (*Id.* ¶¶ 48–49.) And the third category includes three public statements—two on January 3, 2018, and one on January 8, 2018—explaining the very low risk that malicious actors could exploit Spectre Variant 2 on AMD processors. (*Id.* ¶¶ 58–59, 62.) For all three categories, Plaintiffs fail to demonstrate how any challenged statement "affirmatively create[d] an impression of a state of affairs that differ[ed] in a material way from the one that actually exists." *Brody*, 280 F.3d at 1006.

1. AMD's SEC Filings Disclosed Risks Associated with Potential Security Vulnerabilities and Were Not Materially False or Misleading

AMD's SEC filings do not contain a false or misleading statement about Spectre, and Plaintiffs do not allege otherwise. Moreover, AMD repeatedly disclosed the risk that it could face liability in connection with potential third-party attacks on its processors.

Plaintiffs challenge four SEC filings. The first is a Form 8-K filed on July 25, 2017, that attached as exhibits a press release disclosing AMD's financial results for the quarter ending July 1, 2017, and a commentary on AMD's second-quarter results. (CAC ¶ 51.) Both exhibits

expressly incorporate the risk disclosures in AMD's Form 10-Q filed on May 8, 2017. (*Id.*) Specifically, the July 25, 2017 Form 8-K included a cautionary statement urging investors "to review in detail the risks and uncertainties in AMD's Securities and Exchange Commission filings, including but not limited to AMD's Quarterly Report on Form 10-Q for the quarter ended April 1, 2017." (*Id.*) The other three SEC filings Plaintiffs challenge are AMD's May 8, 2017 Form 10-Q, (*id.* ¶ 52); a Form 10-Q filed on August 3, 2017, reporting for the quarter ending June 30, 2017, (*id.* ¶ 54); and a Form 10-Q filed on November 2, 2017, reporting for the quarter ending September 30, 2017. (*Id.* ¶ 56.) Each of these 10-Qs includes the same disclosure: "[AMD] could be subject to potential claims for damages resulting from loss of data from alleged vulnerabilities in the security of our processors." (*Id.* ¶¶ 52, 54, 56.)

Plaintiffs fail to identify specifically anything false or misleading about these statements. The world has many bad actors looking for potential exploits; AMD disclosed that a ***successful*** attack could be harmful to the company. The CAC does not allege that Spectre has ever actually been exploited in the "public domain" to gain access to end-user data on an AMD processor. (*Cf. id.* ¶ 58.) No contemporaneous facts are alleged to demonstrate that AMD was anticipating a successful attack. Plaintiffs' "failure to explain why potential disclosures were inadequate constitutes a failure to satisfy the particularity requirements of the PSLRA." *See, e.g.*, *In re Manulife Fin. Corp. Sec. Litig.*, 276 F.R.D. 87, 100 (S.D.N.Y. 2011) (assessing disclosure of risks associated with equity exposure). Plaintiffs' Section 10(b) claim fails under Rule 9(b) and the PSLRA for this reason alone.

Although it is not stated directly in the CAC, Plaintiffs seem to imply that AMD's SEC filings were incomplete, presumably because they did not disclose more details about how AMD's processors were allegedly susceptible to Spectre, according to GPZ's report. No such disclosure was required. "[A] 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; *see also In re Intuitive Surgical Sec. Litig.*, 65 F. Supp. 3d 821, 836 (N.D. Cal. 2014) (Davila, J.) ("[T]hat the statements were not wholly complete does not necessarily render them misleading to the reasonable investor.").

While Plaintiffs allege that AMD knew about Spectre, (CAC ¶¶ 53, 55, 57), they do not allege (i) that Spectre has ever been used to launch a real-world attack on an AMD processor; (ii) that, during the class period, Defendants had information that a real-world attack was likely despite AMD processors' unique architecture; or (iii) that, during the class period, Defendants were presented with facts showing that a real-world Spectre attack was likely to occur before mitigations could be implemented, if needed, as contemplated by the responsible disclosure principles and the ISO Protocol. If anything, the allegations in the CAC are the opposite of what is required under the PSLRA. (*Id.* ¶ 58 ("The described threat [Spectre] has not been seen in the public domain. When AMD learned that researchers had discovered a new CPU attack targeting the speculative execution functionality . . . we immediately engaged across the ecosystem to address the teams' findings."); *id.* (noting that Variant 1 would be "[r]esolved by software / OS updates" and that Variant 2 posed a "near zero risk of exploitation"); *id.* ¶ 65 (discussing the development of "processor microcode updates and OS patches that [AMD] will make available to AMD customers and partners to further mitigate the threat" of Variant 2).)

Without factual allegations that Defendants knew a successful Spectre attack was likely against AMD's processors before any necessary mitigations were developed and implemented, Plaintiffs fail to plead that the challenged statements are misleading. "Inherent in the concept of falsity is the requirement of contemporaneousness." *City of Roseville Emps.' Ret. Sys. v. Sterling Fin. Corp.*, 963 F. Supp. 2d 1092, 1109 (E.D. Wash. 2013), *aff'd*, 691 F. App'x 393 (9th Cir. 2017). As one court in the Northern District recently explained in the pharmaceutical context, the potential for an adverse event is not enough to render statements false or misleading or to create a duty to disclose. *See In re Dynavax Sec. Litig.*, 2018 WL 2554472, at *6–7 (N.D. Cal. June 4, 2018), appeal docketed, *Kwok Pang v. Dynavax Techs. Corp.*, No. 18-16250 (9th Cir. July 6, 2018). More is needed, such as contemporaneous possession of "information that plausibly indicate[s] a reliable" danger or knowledge that the potential for an adverse event could pose specific harm to the company. *Id.* (dismissing complaint "bereft of allegations that the FDA had indicated that the cardiac events data would halt the approval timeline"); *see also Ong v. Chipotle Mexican Grill, Inc.*, 294 F. Supp. 3d 199, 229 (S.D.N.Y. 2018) (distinguishing "probable,

imminent risks" from speculative risks).

Plaintiffs also fail to explain how investors could have been misled. Again, AMD's filings warned investors that it could be subject to potential damages claims for loss of data stemming from successful third-party attacks on its processors. (CAC ¶¶ 52, 54, 56.) Thus, AMD accurately conveyed the then-current state of affairs—that an exploitation could lead to data loss and result in damages claims if a malicious actor's attacks were successful. *See In re Intuitive Surgical Sec. Litig.*, 65 F. Supp. 3d at 836 (Davila, J.) (granting motion to dismiss where defendants omitted "specific details such as the number of products liability lawsuits made against them," but satisfied disclosure obligation with statement that they could be subject to products liability lawsuits). Nothing else was required, and any additional factual information about Spectre, specifically, could have sent a signal to malicious actors to redouble their efforts and take aim at AMD processors. (*See* Ex. 1.)

It is also noteworthy that the SEC has declined to require specific disclosures related to speculative security threats, particularly where additional disclosure could result in greater risk of exploitation. In 2011, staff at the SEC's Division of Corporation Finance published interpretive guidance to assist public companies in preparing disclosures about cybersecurity risks and incidents. (*See* Ex. 8.) The guidance clarified that the "federal securities laws do not require disclosure that itself would compromise a registrant's cybersecurity. Instead, registrants should provide sufficient disclosure to allow investors to appreciate the nature of the risks faced by the particular registrant in a manner that would not have that consequence." (*Id.* at 3.)[5] AMD did just that by disclosing the risk of liability stemming from exploits aimed at its processors. Providing further detail about a theoretical vulnerability that Plaintiffs do not allege has been exploited in the real world more than a year later could have handed bad actors a roadmap to a

[5] These statements—which provided guidance during the period at issue—are persuasive interpretations of applicable securities laws. *See In re NVIDIA Corp. Sec. Litig.*, 768 F.3d at 1055 (considering an SEC interpretive release in affirming a grant of defendants' motion to dismiss); *Ganino v. Citizens Utils. Co.*, 228 F.3d 154, 163 (2d Cir. 2000) (considering an SEC staff accounting bulletin as "persuasive guidance" in evaluating a 10(b) claim); *see also SEC v. Aline Sec. Corp.*, 308 F. Supp. 3d 775, 789 (S.D.N.Y. 2018) (explaining the various levels of deference courts grant to agency guidance).

potential exploit. (*Id.* at 1.) And such a hasty disclosure would have been contrary to accepted industry practice and the ISO Protocol.

2. AMD's Press Release on Ryzen Products Was Not Materially False or Misleading

Plaintiffs claim that a press release highlighting various Ryzen security features was false and misleading, supposedly because AMD knew about the possibility of Spectre and the theoretical security threats a successful exploit may have posed. (CAC ¶¶ 49–50.)[6] But many of the statements Plaintiffs challenge are immaterial because they are not verifiable statements of fact. (*See, e.g.*, *id.* ¶ 48 ("Ryzen . . . will bring reliability, security and performance to enterprise desktops worldwide."); *id.* ("state-of-the-art silicon-level security"); *id.* ¶ 49 ("transparent secure memory encryption").) Courts routinely find that these types of statements are immaterial opinions that do not sway investors and are insufficient to state a Section 10(b) claim as a matter of law. *See, e.g.*, *Kelly v. Elec. Arts, Inc.*, 2015 WL 1967233, at *7 (N.D. Cal. Apr. 30, 2015) ("[T]he term 'de-risk' is a non-actionable vague expression of corporate optimism and puffery."); *Shemian v. Research In Motion Ltd.*, 2013 WL 1285779, at *6, 20–23 (S.D.N.Y. Mar. 29, 2013) (praising products in general terms—by referencing, for example, "advanced security features"—was "too vague and inconsequential to give rise to any duty to disclose"), *aff'd*, 570 F. App'x 32 (2d Cir. 2014); *In re Splash Tech. Holdings, Inc. Sec. Litig.*, 160 F. Supp. 2d 1059, 1077 (N.D. Cal. 2001) (finding statements using the words "strong," "robust," "well positioned," "solid," and "improved" to be "vague and nonactionable").

As to other statements about security features, like Ryzen provides "secure boot [and] OS

[6] Plaintiffs also cite a Ryzen product "review" and a video discussing security features of AMD's products. (*See* CAC ¶¶ 32, 34 ("Security is going to be one of the big pillars within AMD," and "Ryzen Pro chips all come with a dedicated security processor within the CPU," referencing AMD's "secure boot process.").) Plaintiffs do not include the review or the video in their "False and Misleading Statements" allegations. To the extent that Plaintiffs claim these are actionable misstatements, however, that claim would fail based on the same deficiencies discussed throughout—e.g., Plaintiffs fail to allege they were false, explain why they were misleading, demonstrate their materiality, or attribute them to any Defendant. Regarding the video, specifically, the engineer's comments about data protection refer to a particular security feature applicable when data moves from a server to the cloud. (*Id.* ¶ 34.) Plaintiffs do not allege that this feature is potentially impacted by Spectre.

and application independent DRAM encryption without requiring software modifications," (CAC ¶¶ 48–49), the CAC fails to allege facts demonstrating how or why they are factually inaccurate or misleading. *See In re GlenFed, Inc. Sec. Litig.*, 42 F.3d at 1548 ("[P]laintiff must set forth what is false or misleading about a statement, and why it is false."). Plaintiffs imply that AMD's June 29, 2017 press release[7] was incomplete because it did not include additional details about Spectre. (CAC ¶ 50.) But as demonstrated above, simply alleging an incomplete statement is not enough. Section 10(b) does not contain a "freestanding completeness requirement." *Brody*, 280 F.3d at 1006. This is because "[n]o matter how detailed and accurate disclosure statements are, there are likely to be additional details that could have been disclosed but were not." *Id.*

Here, Plaintiffs fail to show how the statements are actionable. *Id.* For example, Plaintiffs do not allege that AMD affirmatively stated its processors were impervious to security vulnerabilities. To the contrary, the press release posted on AMD's website expressly incorporated the risk disclosures from AMD's May 8, 2017 SEC filing—a fact conspicuously omitted from the CAC—which warn that AMD "could be subject to potential claims for damages resulting from loss of data from alleged vulnerabilities in the security of our processors."[8] (Ex. 7; *see also* CAC ¶ 52.) By qualifying the security features mentioned in the press release with the risk disclosures it incorporated by reference, AMD communicated the state of affairs accurately. And Ninth Circuit case law is in agreement that where a company advertises security features without "promis[ing] perfect service," its statements are not actionable despite specific, undisclosed potential issues where the "total mix of information" would not mislead a reasonable investor. *In re LifeLock, Inc. Sec. Litig.*, 690 F. App'x 947, 953 (9th Cir. 2017) (no misleading omission where defendant touted its anti-theft protection services but made no representation of "perfect service"); *see also Brody*, 280 F.3d at 1006 (no misleading omission where the press release did not suggest merger was imminent).

Plaintiffs also fail to explain how general statements about product security or specific

[7] Unless otherwise stated, references to the "press release" apply equally to the presentation Plaintiffs allege accompanied AMD's June 29, 2017 press release. (CAC ¶ 48.)

[8] Given that the press release was issued with the "accompanying presentation," (*id.* ¶ 48), the press release's incorporation of risk disclosures applied equally to the presentation.

statements about security features unrelated to speculative execution have any relationship to Spectre. For example, nowhere in the CAC do Plaintiffs allege that the security features noted in the press release were not, in fact, present. Nor do they allege that these features were, or could have been, affected by Spectre. Instead, as alleged by Plaintiffs, Spectre is a theoretical vulnerability with no real-world application to date. (*Cf.* CAC ¶ 58.) Given these deficiencies in the CAC, Plaintiffs fail to satisfy the PSLRA's heightened pleading requirement, and, as this Court has held on multiple occasions, their Section 10(b) claim as to the press release must be dismissed as a result. *See, e.g.*, *In re VeriFone Sec. Litig.*, 2014 WL 3920322, at *4 (N.D. Cal. Aug. 8, 2014) (Davila, J.) (finding that plaintiffs failed to allege false and misleading misstatements or omissions under the PSLRA where they did not "provide specific facts or reasons to show how each statement was false or misleading"); *see also Metzler*, 540 F.3d at 1070 ("A litany of alleged false statements, unaccompanied by the pleading of specific facts indicating why those statements were false, does not meet [the PSLRA pleading] standard.").

Even if the June 29, 2017 press release could be viewed as an actionable statement, the claim against the Individual Defendants must still be dismissed because Plaintiffs make no attempt to connect the Individual Defendants to the press release. To be held personally liable under Section 10(b), an individual must have been the maker of the alleged misstatement, either by having the statement attributed to him or her or controlling the content and communication of the statements. *See Janus Capital Grp., Inc. v. First Derivative Traders*, 564 U.S. 135, 142–43 (2011). Moreover, to satisfy Rule 9(b)'s heightened pleading standard, Plaintiffs' allegations must contain not only "an account of the time, place, and specific content of the false representations," but also "***the identities of the parties to the misrepresentations***." *In re VeriFone Sec. Litig.*, 2014 WL 3920322, at *3 (quoting *Swartz v. KPMG LLP*, 476 F.3d 756, 764 (9th Cir. 2007)) (emphasis added). Plaintiffs provide no such identities, and they do not allege that Dr. Su or Mr. Kumar was involved with drafting or disseminating this statement, or had any reason to think it should include information about Spectre.

3. AMD's January 2018 Statements About Spectre Were Not Materially False or Misleading

Finally, while Plaintiffs claim that three public statements made in early January about Spectre should result in liability for securities fraud, none is sufficient to support a Section 10(b) claim. (*See* CAC ¶¶ 60, 63.) The first is an unattributed January 3, 2018 website post in which AMD responded to GPZ's announcement, explained that it was unaware of any successful exploitation in the public domain, and noted that Variant 2 posed a "near zero risk of exploitation" on AMD's processors. (*Id.* ¶ 58.) The second statement, allegedly made by an unidentified "spokesperson" on January 3, 2018, similarly noted that Variant 2 posed a "near zero risk" of vulnerability as applied to AMD's processors. (*Id.* ¶ 59.) The third statement was made by Dr. Su on January 8, 2018, during a CNBC interview in which she said that Variant 2 would be "difficult to access"—i.e., difficult to exploit—and that a Variant 2 exploitation on an AMD processor would be "rare." (*Id.* ¶ 62.) Each of these statements, Plaintiffs claim, was misleading because, in a January 11, 2018 public statement, AMD said that while "Variant 2 . . . is applicable to AMD processors . . . AMD's processor architectures make it difficult to exploit Variant 2," (*id.* ¶ 65), and Dr. Su said during an interview on the same day that AMD was theoretically susceptible to both variants. (*Id.* ¶ 66.) Plaintiffs also claim that, as to the January 3 statements, Defendants "knew" that the risk of exploitation from Variant 2 was "material." (*Id.* ¶ 60.)

Plaintiffs, however, allege no facts showing that Defendants were aware in early January of anything to suggest that the risks of a successful Spectre exploit were greater than what was disclosed in the January 3 and January 8 public statements. *In re GlenFed, Inc. Sec. Litig.*, 42 F.3d at 1549 (plaintiff must explain "why the disputed statement was untrue or misleading ***when made***"). In fact, more than a year after GPZ allegedly alerted AMD to Spectre, Plaintiffs do not allege there has been a single real-world exploitation of Variant 2 against an AMD processor. (*Cf.* CAC ¶ 58.) Under those circumstances, AMD's January 2018 statements cannot plausibly be seen as materially false or misleading. Additionally, Plaintiffs acknowledge AMD's public statements that AMD (i) acted quickly to address GPZ's findings, (ii) developed mitigations for Variant 1, and (iii) accurately assessed the minimal risk posed by Variant 2. (*Id.* ¶¶ 58–59, 62,

65–66.) The CAC therefore fails to demonstrate that Defendants' knowledge at the time was inconsistent with their statements about Spectre.

Moreover, even a cursory review of AMD's January 3 and 8 statements reveals that they are entirely consistent with each other, as well as with the January 11 statements. Plaintiffs' theory is premised on semantic gamesmanship—the faulty notion that saying Variant 2 posed a "near zero risk" to AMD's processors, (*id.* ¶¶ 58–59), or that it was difficult to exploit, (*id.* ¶ 62), somehow equated to saying that Variant 2 was ***never*** a threat to AMD's processors. A "***near*** zero risk" necessarily implicates some level of risk. The January 11 statement was in no way inconsistent with the January 3 statements; none of the statements said or implied that AMD's processors were immune to Variant 2 attacks. Nor was the January 11 statement inconsistent with Dr. Su's January 8 statement; they were virtually identical in relevant part. Dr. Su's January 8 statement noted that Variant 2 would be "difficult to access" in the real world, (*id.* ¶ 62), and the January 11 statement noted that Variant 2 would be "difficult to exploit." (*Id.* ¶ 65.)

This consistency belies any claim that the January 3 and 8 statements somehow misrepresented the likelihood that a bad actor could successfully exploit Variant 2 on an AMD processor. "[T]he disclosure required by the securities laws is measured . . . by the ability of the material to accurately inform rather than mislead." *In re Intuitive Surgical Sec. Litig.*, 65 F. Supp. 3d at 835 (quoting *In re Convergent Tech. Sec. Litig.*, 948 F.2d 507, 512 (9th Cir. 1991)). Here, each of the January statements accurately informed the public of the potential—if highly unlikely—that Variant 2 could be exploited. Thus, none of Defendants' statements were "contradictory or necessarily inconsistent." *See In re Read-Rite Corp.*, 335 F.3d 843, 846–48 (9th Cir. 2003), *abrogated on other grounds as recognized in S. Ferry LP, No. 2 v. Killinger*, 542 F.3d 776, 782–84 (9th Cir. 2008). Securities fraud claims require much more than slight differences in language used to communicate judgments about the technical risks of a theoretical exploit that is not alleged to have been successfully practiced in the real world. *See, e.g.*, *In re Yahoo! Inc. Sec. Litig.*, 611 F. App'x 387, 389 (9th Cir. 2015) (statement not misleading because "the information disclosed was 'entirely consistent with the more detailed explanation'" that plaintiffs alleged should have been disclosed).

Additionally, with the exception of Dr. Su's January 8 statement on CNBC, Plaintiffs make no attempt to connect the Individual Defendants with the January statements. This is a separate ground for dismissing Mr. Kumar from all claims regarding these statements and Dr. Su from all claims based on AMD's unattributed January 3 and January 11 statements.

4. Plaintiffs' Allegations and Judicially Noticeable Facts Demonstrate That Spectre Was Not Material to Investors

The Court should also dismiss the Section 10(b) claim because Plaintiffs fail to establish that Spectre was material to investors. To be material, there must be 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." *TSC Indus., Inc. v. Northway, Inc.*, 426 U.S. 438, 449 (1976). And an allegedly misleading statement must be "read in conjunction with the surrounding language, not in a vacuum." *Mallen II*, 2013 WL 1294640, at *8. This is a high bar; a materiality "standard that is too low would bury the shareholders in an avalanche of trivial information—a result that is hardly conducive to informed decisionmaking." *Retail Wholesale & Dep't Store Union Local 338 Ret. Fund v. Hewlett-Packard Co.*, 845 F.3d 1268, 1277 (9th Cir. 2017).

That AMD received a report about a potential security vulnerability is unremarkable. (*See* Ex. 9.) AMD's disclosures already put investors on notice that it could potentially face liability for data loss if malicious attacks on its processors were successful. The market was aware of the responsible disclosure principle, which had made its way into the ISO Protocol that had been in place for years. (*See* Ex. 1.) And any technology user is aware of the possibility that security vulnerabilities exist and malicious attacks occur. (*See* CAC ¶¶ 48–49 (marketing security features intended to mitigate security risks).)

Further, Plaintiffs do not allege that Spectre has been actively exploited by any bad actor, and nothing in the CAC suggests that successful exploitation is or was imminent at the time AMD made any statement at issue in the CAC. Simply put, AMD received a report of a possible security vulnerability, like the many identified each year, (*see, e.g.*, Ex. 9), and worked to test and address it. (*See* CAC ¶¶ 58, 62, 65.) AMD "need not detail every corporate event, current or

prospective . . .” *Marx v. Comput. Scis. Corp.*, 507 F.2d 485, 491 (9th Cir. 1974). Doing so would inundate shareholders and make informed decision making unnecessarily difficult to accomplish, especially where the ordinary investor is already aware of such risks, both through public disclosures and common knowledge. *See TSC Indus.*, 426 U.S. at 448–49.

Plaintiffs have failed to allege any significant financial impact related to any of the challenged statements—the SEC filings, the press release, or the January 2018 statements about Spectre. In fact, AMD’s stock price ***increased*** between Spectre’s announcement and the final day of the class period, when Plaintiffs allege that the “truth” was revealed to the market. (*See* Ex. 2.) Where, as here, “the financial import of alleged misstatements is *de minimis*, those alleged misstatements are immaterial as a matter of law.” *In re Hansen Nat. Corp. Sec. Litig.*, 527 F. Supp. 2d 1142, 1161 (C.D. Cal. 2007). No facts are alleged to render Spectre or its disclosure financially material to AMD, and without factual allegations, Plaintiffs’ conclusory labels must be ignored. As one court in this District explained, “[i]f a misrepresentation is deemed material simply because it is a misrepresentation, then the law’s materiality requirement is altogether meaningless.” *SEC v. Reyes*, 491 F. Supp. 2d 906, 912 n.6 (N.D. Cal. 2007).

B. Plaintiffs Fail to Plead Any Inference of Scienter

Also fatal to the CAC is its failure to allege facts from which the Court can draw a “strong inference” of scienter. *Tellabs*, 551 U.S. at 321–22. To qualify as “strong,” 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.” *Id*. at 314. But here, the CAC contains no theory of fraudulent intent, much less a cogent and compelling one supported by particularized factual allegations. Indeed, despite devoting 94 paragraphs to their other allegations, Plaintiffs use only two to discuss scienter, and even then Plaintiffs fail to allege ***any*** specific facts that would satisfy the PSLRA. (CAC ¶¶ 83–84.) The most Plaintiffs can muster are conclusory allegations that merely recite the legal standard. (*See, e.g.*, *id.* ¶ 83 (“Defendants . . . knew that the public documents and statements . . . were materially false and misleading”); *id.* ¶ 84 (“Individual Defendants . . . had actual knowledge . . . and intended to deceive . . . or, in the alternative, acted with reckless disregard for the truth”).) Courts in the Ninth Circuit routinely

reject boilerplate allegations like those in the CAC. *See Brown v. China Integrated Energy, Inc.*, 875 F. Supp. 2d 1096, 1121 (C.D. Cal. 2012) (rejecting similar recitations of legal standard); *see also Mohebbi v. Khazen*, 50 F. Supp. 3d 1234, 1252 (2014) ("Conclusory statements about Defendants' scienter, without corroborating factual allegations, are usually insufficient, standing alone, to adequately allege scienter.").

Plaintiffs do not allege any illicit motive for declining to publicize a potential security vulnerability until mitigations were in place. Delaying publication until whatever needed mitigations are prepared is widely viewed as a "best practice" in the technology and software industries, consistent with the ISO Protocol and the best interest of end users. (*See* Ex. 1; CAC ¶ 38 (citing GPZ's policy for reporting vulnerabilities "typically once a patch is available").) The Court "must take into account plausible opposing inferences," including that the Defendants made a reasonable judgment to follow industry standards and the ISO Protocol. *See Tellabs*, 551 U.S. at 323.

The allegations here are controlled by the Ninth Circuit's decision in *In re NVIDIA Corp. Securities Litigation*. In that case, the Ninth Circuit found that a disclosure approach much like AMD's created no compelling inference of fraudulent intent. There, NVIDIA disclosed defects in its chips to investors, took a $196 million charge to earnings, and saw its stock price drop 31%. 768 F.3d at 1050–51. NVIDIA was first advised of the defect approximately one year earlier. *Id.* at 1051. The Ninth Circuit rejected the plaintiffs' argument that NVIDIA intentionally misled investors by waiting to disclose its defect until it had prepared replacement products. *Id.* at 1057. The court held that the more compelling inference was that "NVIDIA was first investigating the root cause, and then the scope" of the defect before disclosing it. *Id.* at 1056. Plaintiffs were unable to allege scienter on these facts. *Id.*

So too here, where there are ***no*** specific facts suggesting Defendants acted with an intent to defraud or that the supposedly undisclosed security vulnerability actually had an impact on the company's financial statements. Rather, the allegations in the CAC demonstrate the opposite—that AMD respected responsible disclosure principles by first researching Spectre's theoretical applications and developing mitigations, where appropriate, before talking about it publicly,

while also continuing to disclose to investors that AMD faced a risk of liability stemming from third-party attacks on its processors. (*See, e.g.*, CAC ¶¶ 52, 54, 56, 58.) And the facts here are even more favorable to AMD than they were in *NVIDIA*: Plaintiffs allege only a minimal and fleeting stock price decline as a result of the ultimate "disclosure."

As discussed above, Plaintiffs also fail to allege that Defendants were aware of any actual or imminent real-world exploits of Spectre during the class period. Nor do Plaintiffs allege that Defendants had reason to believe there ***would*** be a Spectre-related attack. The allegations suggest no facts to indicate that Spectre should have been handled any differently than any other potential security threat: assessment, followed by mitigation, if needed, before successful exploit, and then disclosure. And Plaintiffs do not allege that AMD was wrong about the low likelihood of either Spectre variant affecting AMD's processors—either as a result of successful mitigations or because AMD processors' architecture impeded Spectre's risk. There are simply no allegations "to indicate that the [public] statements made did not reflect the honest belief of the authors.'" *In re AstraZeneca Sec. Litig.*, 559 F. Supp. 2d 453, 471–72 (S.D.N.Y. 2008), *aff'd sub nom. State Univs. Ret. Sys. of Ill. v. AstraZeneca PLC*, 334 F. App'x 404 (2d Cir. 2009) (finding no allegations of scienter where it was "not unreasonable for defendants to believe in their product"). Accordingly, the CAC offers no allegation to create a strong inference of fraudulent intent.

The Ninth Circuit also requires Plaintiffs to "allege scienter with respect to each of the individual defendants" where, as here, Plaintiffs "seek to hold individuals and a company liable on a securities fraud theory." *Or. Pub. Emps. Ret. Fund v. Apollo Grp. Inc.*, 774 F.3d 598, 607 (9th Cir. 2014). Again, the CAC fails. Plaintiffs cannot attribute a wrongful state of mind to Dr. Su and Mr. Kumar simply because they served as CEO and CFO, respectively. The PSLRA requires a plaintiff to plead specific facts; "accusations founded on nothing more than a defendant's corporate position are entitled to no weight." *Plumbers & Steamfitters Local 773 Pension Fund v. Canadian Imperial Bank of Commerce*, 694 F. Supp. 2d 287, 300 (S.D.N.Y. 2010). Plaintiffs allege nothing else, dooming their CAC. *See, e.g.*, *Brodsky*, 630 F. Supp. 2d at 1118 (rejecting plaintiffs' scienter allegations that defendants must have known about misrepresentations due to positions as Chairman, CEO, and CFO); *also In re U.S. Aggregates,*

Inc. Sec. Litig., 235 F. Supp. 2d 1063, 1074 (N.D. Cal. 2002) ("[P]laintiffs must do more than allege that these key officers had the requisite knowledge by virtue of their 'hands on' positions.") (quotation, citation omitted).

Similarly, Plaintiffs' allegations that the Individual Defendants signed several public filings, including Sarbanes-Oxley certifications, standing alone, cannot support a Section 10(b) claim. (CAC ¶¶ 52 n.19, 54 n.20, 56 n.21.) It is well established that merely signing such documents is insufficient to raise a strong inference of scienter. *Zucco*, 552 F.3d at 1003–04. Indeed, if signing a Sarbanes-Oxley certification were enough, then "scienter would be established in every case . . . thereby eviscerating the pleading requirements for scienter set forth in the PSLRA." *Garfield v. NDC Health Corp.*, 466 F.3d 1255, 1266 (11th Cir. 2006); *see also Glazer Capital Mgmt., LP v. Magistri*, 549 F.3d 736, 747 (9th Cir. 2008) (adopting holding of *Garfield* and finding no strong inference of scienter based on Sarbanes-Oxley certification). Moreover, Plaintiffs' attempt to lump the Individual Defendants together, (*see* CAC ¶ 18), is precisely the type of "group pleading" that courts in the Ninth Circuit routinely reject in light of the heightened pleading requirements for scienter. *See, e.g.*, *Lapiner v. Camtek, Ltd.*, 2011 WL 445849, at *3 (N.D. Cal. Feb. 2, 2011) (noting that the "majority of district courts within the Ninth Circuit have concluded that group pleading is no longer viable"); *In re Hansen Nat. Corp. Sec. Litig.*, 527 F. Supp. 2d at 1153–54 (same); *see also Glazer Capital*, 549 F.3d at 745 (holding that PSLRA requires plaintiff to plead "in great detail" facts that show scienter as to each individual and granting defendant CEO's dismissal motion).

In sum, while Plaintiffs allege generally that AMD knew about Spectre, there are simply no allegations raising a strong inference that any Defendant intended to "deceive, manipulate, or defraud." *Ernst & Ernst*, 425 U.S. at 193 n.12. "[K]nowing about the existence of [problems] and knowing that one should report these [problems] to the public are two different things." *Colyer v. Acelrx Pharm., Inc.*, 2015 WL 7566809, at *13 (N.D. Cal. Nov. 25, 2015). The most cogent and logical explanation is that AMD disclosed enough public information to give reasonable investors an accurate impression of the state of affairs, *Brody*, 280 F.3d at 1006, avoided disclosure of detailed information that might embolden bad actors seeking to penetrate

AMD's processors, (*see, e.g.*, Ex. 8), and respected the principles of responsible disclosure by taking time to research and develop mitigations, where appropriate, before publicizing specific details about Spectre.

C. The CAC Fails to State a Section 20 Claim Against Dr. Su and Mr. Kumar

Because Plaintiffs fail to state a Section 10(b) claim, Plaintiffs' Section 20 claim necessarily fails. *Zucco*, 552 F.3d at 990 ("Section 20(a) claims may be dismissed summarily . . . if a plaintiff fails to adequately plead a primary violation of Section 10(b)."). The Court should dismiss the control-person claims for the independent reason that the CAC fails to allege with the requisite specificity that any Individual Defendant exercised actual power or control over AMD's public statements about Spectre. *See* 15 U.S.C. § 78t(a). Instead, the CAC offers only generalized allegations that the Individual Defendants held high-level positions and signed AMD's SEC filings, (*see* CAC ¶¶ 19, 52 n.19, 54 n.20, 56 n.21), unremarkable observations that are insufficient to state a claim as a matter of law. *See, e.g.*, *Bruce v. Suntech Power Holdings Co.*, 2013 WL 6843610, at *9 (N.D. Cal. Dec. 26, 2013) (dismissing Section 20 claim against CFO based on "conclusory allegations of his involvement in the day-to-day operations" and "standard Sarbanes–Oxley certifications, standing alone"); *In re Downey Sec. Litig.*, 2009 WL 736802, at *15 (C.D. Cal. Mar. 18, 2009) (rejecting "boilerplate allegation[s]" based on positions and stock ownership).

IV. CONCLUSION

For all of the foregoing reasons, AMD respectfully requests that the Court dismiss Plaintiffs' CAC with prejudice.

Dated: September 25, 2018

O'MELVENY & MYERS LLP
MATTHEW W. CLOSE
BRITTANY ROGERS

By: /s/ Matthew W. Close
Matthew W. Close

Attorneys for Defendants
Advanced Micro Devices, Inc.,
Lisa T. Su, and Devinder Kumar