United States District Court
Northern District of California

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

DIANA HAUCK, et al.,

Plaintiffs,

v.

ADVANCED MICRO DEVICES, INC.,

Defendant.

Case No. 18-CV-00447-LHK

ORDER GRANTING AMD'S MOTION TO DISMISS PLAINTIFFS' SECOND CONSOLIDATED AMENDED COMPLAINT WITH PREJUDICE

Re: Dkt. No. 97

Plaintiffs Diana Hauck, Shon Elliott, Michael Garcia, JoAnn Martinelli, Benjamin Pollack, Jonathan Caskey-Medina (collectively, "Plaintiffs") bring suit individually and on behalf of various putative classes against Defendant Advanced Micro Devices, Inc. ("AMD"). Plaintiffs assert claims relating to AMD's manufacture and sale of central processing units ("CPUs" or "processors") that purportedly contain cybersecurity flaws. The parties elected to litigate through summary judgment eight claims, seven of which Plaintiffs reallege in the second consolidated amended complaint ("SCAC"). Before the Court is AMD's motion to dismiss those seven claims. Having considered the parties' submissions, the relevant law, and the record in this case, the Court GRANTS AMD's motion to dismiss with prejudice all seven of Plaintiffs' claims.

I. BACKGROUND

A. Factual Background

AMD designs, manufactures, sells, and distributes central processing units ("CPUs" or "processors"). *See* ECF No. 95 ("SCAC") ¶ 34. AMD's processors are incorporated into end-consumer products such as computers and servers, and are also sold as stand-alone items. *Id.* at ¶ 39. Plaintiffs all purchased AMD's processors either in end-consumer products or as stand-alone items. *Id.* at ¶¶ 8–33.

CPU speed is an element of a consumer's decision to purchase a processor, as sufficient processing speed is necessary to effectively operate a computer's software programs and hardware. *Id.* at ¶ 63. CPU speed is measured in terms of clock speed—the greater the clock speed, the greater the CPU's processing speed. *Id.* at ¶ 64. Broadly, to increase clock speed, modern processors usually implement techniques called branch prediction, speculative execution, and caches. *Id.* at ¶¶ 53–60. AMD's implementation of these three techniques in the microarchitecture of its products exposes users to "security vulnerabilities." *Id.* at ¶ 61.

In a section of the SCAC called "The Defect Explained," Plaintiffs allege that "AMD's use of branch prediction, speculative execution, and caches in its CPU designs . . . created an inherent defect in the CPU that compromised consumers' most sensitive information." *Id.* at ¶ 107.

In June 2017, a third party, Google Project Zero, disclosed to AMD the existence of a vulnerability that attackers could use to exploit AMD's processors. *Id.* at ¶ 163. "Mis-speculation is a normal function of the CPU when its branch predictor has incorrectly 'guessed' the next instructions the CPU needs to execute and the CPU speculatively executes instructions down the mispredicted path." *Id.* at ¶ 113. Plaintiffs describe the vulnerability that Google Project Zero disclosed to AMD in June 2017 as: "both the speculative execution process and the branch predictor in AMD's CPUs can be coerced by an attacker to speculatively execute unnecessary instructions hand-picked by the attacker, leading to intentional mis-speculation." *Id.* at ¶¶ 113, 163. *Id.* An attacker can use such intentional mis-speculation to reveal a CPU user's personal information. *Id.* at ¶¶ 113–14. Beginning on January 2, 2018, journalists published articles that

disclosed to the public that the mis-speculation vulnerability could exploit AMD's processors, as well as processors manufactured by other companies, including Intel. *Id.* at ¶¶ 161–62.

In Plaintiffs' consolidated amended complaint ("CAC"), Plaintiffs referred to this mis-speculation vulnerability as Spectre. The CAC described Spectre as: "To exploit a high-speed CPU's speculative execution capability, an attacker writes a piece of malicious code that causes the processor to 'mispredict' the result of a branch instruction, inducing the CPU to speculatively execute instructions that it otherwise would not execute." ECF No. 53 at ¶ 14. The CAC further alleged, "It is these speculative instructions, executed on the mispredicted path, that leak the information that the attacker is then able to recover." *Id.* The CAC stated that Google Project Zero disclosed Spectre to AMD in June 2017 and that journalists disclosed Spectre to the public beginning on January 2, 2018. *Id.* at 17, ¶¶ 84. Plaintiffs' CAC defined the Defect as "20 years [of] serious security vulnerabilities," *id.* at ¶ 1, but then referred to Spectre as the Defect. For example, Plaintiffs alleged that "Defendant knowingly sold or leased a defective product without informing customers about the Spectre Defect." *Id.* at ¶ 484. As discussed below, Plaintiffs' SCAC deletes all mention of the name Spectre, but continues to describe the mis-speculation vulnerability in terms identical to the CAC's description of Spectre.

Later in January 2018, operating system companies, including Microsoft, released security "patches" intended to mitigate the mis-speculation vulnerability. *Id.* at ¶¶ 160, 165. Plaintiffs do not allege that AMD developed or released any anti-Spectre patches. These third-party patches can slow down a CPU's processing speed. *Id.* at ¶¶ 171–72. For example, Plaintiff Diana Hauck alleges that she installed a patch after learning about the mis-speculation vulnerability, but her "processor no longer could achieve its advertised performance level, and her computer frequently crashed, sometimes several times per day." *Id.* at ¶ 10.

Plaintiffs seek to represent a Nationwide Class of "[a]ll persons that purchased or leased one or more AMD processors, or one or more devices containing an AMD processor in the United States within the applicable statute of limitations." *Id.* at ¶ 193. Plaintiffs also seek to represent

various state classes. *Id.*

B. Procedural History

On January 1, 2018, Plaintiffs filed this action. ECF No. 1. On April 9, 2018, this case was consolidated with and related to two later-filed cases. ECF No. 37. On May 23, 2018, the Court ordered Plaintiffs to file a consolidated amended complaint ("CAC") and ordered each side to select four causes of action to litigate through summary judgment. ECF No. 50.

On June 13, 2018, Plaintiffs filed the CAC. ECF No. 53. In the CAC, Plaintiffs alleged 25 causes of action, all relating to the alleged harm suffered by the named Plaintiffs and the putative classes in purchasing AMD chips or products containing them. In brief, Plaintiffs alleged that AMD's implementation of branch prediction and speculative execution in its processors exposes users to the Spectre vulnerability, which Google Project Zero disclosed to AMD in June 2017 and journalists disclosed to the public on January 2, 2018. CAC ¶¶ 17, 58, 67, 84. Plaintiffs defined Spectre as: "To exploit a high-speed CPU's speculative execution capability, an attacker writes a piece of malicious code that causes the processor to 'mispredict' the result of a branch instruction, inducing the CPU to speculatively execute instructions that it otherwise would not execute." *Id.* at ¶ 14. Plaintiffs further alleged, "It is these speculative instructions, executed on the mispredicted path, that leak the information that the attacker is then able to recover. *Id.* Plaintiffs claimed that had they known about Spectre, they would not have purchased the computers or chips or would have paid less for them. *Id.* at ¶¶ 21–26. Plaintiffs also claimed that third-party patches to fix Spectre—patches that AMD did not develop or release—reduce processing speed. *Id.* at ¶ 19.

Plaintiffs elected to litigate four causes of action through summary judgment: (1) Count III—violation of California's Unfair Competition Law ("UCL") for unfair business practices, Cal. Bus. & Prof. Code § 17200 *et seq.*, *id.*; (2) Count V—fraud by omission, *id.*; (3) Count XI—violation of Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), Fla. Stat. § 501.201, *et seq.*, *id.*; and (4) Count XIX—violation of the Massachusetts Consumer Protection Act ("MCPA"), Mass. Gen. Laws ch. 93A § 1, *et seq.*, *id.* ECF No. 54.

AMD also selected four causes of action to litigate through summary judgment: (1) Count VII—breach of express warranty based on representations, Cal. Comm. Code § 2313, *id.*; (2) Count VIII—breach of implied warranty, Cal Comm. Code §§ 2314-15, *id.*; (3) Count X—negligence, *id.*; and (4) Count XVII—warranty against redhibitory defects, La. Civ. Code Ann. Art. 2520, 2524, *id*. ECF No. 61.

On July 13, 2018, AMD filed a motion to dismiss the CAC. ECF No. 64. AMD sought to dismiss seven of Plaintiffs' eight claims that the parties had elected to litigate through summary judgment. *Id.* On September 4, 2018, Plaintiffs filed their opposition. ECF No. 73. AMD replied on September 25, 2018. ECF No. 75. On September 4, 2018, Plaintiff Jonathan Caskey-Medina voluntarily dismissed without prejudice Count XIX, the MCPA claim. ECF No. 72. AMD also requested that the Court take judicial notice of two documents, ECF No. 65, a request Plaintiffs opposed. ECF No. 74.

On October 29, 2018, the Court granted in part, denied in part, and denied in part as moot AMD's motion to dismiss. ECF No. 88 ("MTD Order"). The Court denied without prejudice AMD's motion to dismiss Count IV because the parties had not elected to litigate Count IV. *Id.* at 7. The Court also denied as moot AMD's motion to dismiss Count XIX, the MCPA claim, because Caskey-Medina—the only Massachusetts plaintiff—had voluntarily dismissed the MCPA claim without prejudice. *Id.* The Court also denied as moot AMD's request for judicial notice of two documents because the Court's order did not rely on either document. *Id.* at 5.

The Court dismissed the remainder of Plaintiffs' claims without prejudice. First, the Court dismissed Plaintiffs' FDUTPA fraud claim because Plaintiffs' definitions of "the Defect" failed to satisfy the heightened pleading standard of Federal Rule of Civil Procedure 9(b). *Id.* at 7–10. Plaintiffs' CAC defined the Defect as "20 years [of] serious security vulnerabilities," CAC at ¶ 1, but then referred to Spectre—the mis-speculation vulnerability that Google Project Zero disclosed to AMD in June 2017 and that journalists disclosed to the public on January 2, 2018—as the Defect. For example, Plaintiffs alleged that "Defendant knowingly sold or leased a defective

product without informing customers about the Spectre Defect." *Id.* at ¶ 484. Then, in Plaintiffs' opposition to AMD's motion to dismiss, Plaintiffs claimed that the Defect was not Spectre, but rather "the security vulnerabilities created by AMD's design." ECF No. 73 at 1. However, as the Court explained, "Plaintiffs fail[ed] to identify what security vulnerabilities affected AMD's processors for the last 20 years *other than Spectre* and fail[ed] to explain how AMD's design created those vulnerabilities." MTD Order at 9 (emphasis added). Thus, the Court concluded that "[g]iven Plaintiffs' vague and inconsistent definitions of Defect, AMD can hardly be expected to know exactly what the contents of its alleged misrepresentations are." *Id.* The Court concluded that Plaintiffs' affirmative misrepresentations claim also failed because Plaintiffs failed to plead why AMD's statements about its processors' clock speed were false when made. *Id.* at 9–10.

Second, the Court dismissed Plaintiffs' claim for fraud by omission because Plaintiffs did not allege that AMD knew about any security vulnerability before Plaintiffs purchased the AMD processors. *Id.* at 11. Plaintiffs relied on "vague, sweeping statements about industry research and general knowledge garnered from conferences," which was insufficient to allege AMD's knowledge of any security vulnerability in AMD's processors. *Id.* Plaintiffs alleged only that Google Project Zero disclosed Spectre to AMD in June 2017, *after* Plaintiffs purchased their processors. *Id.* In addition, the Court explained that given Plaintiffs' "multiple definitions" of the Defect, "AMD cannot meaningfully respond to accusations that it omitted information about the Defect because AMD does not know what the Defect is." *Id.*

Third, the Court dismissed Plaintiffs' California claim for breach of express warranty because Plaintiffs failed to plead the exact terms of the warranty and failed to plead harm. *Id.* at 12–14.

Fourth, the Court dismissed Plaintiffs' California claims for breach of the implied warranty of merchantability and breach of the implied warranty of fitness for a particular purpose because Plaintiffs failed to plead that any security vulnerability compromised the basic functionality of AMD's processors and failed to plead that Plaintiffs purchased the processors for a particular

purpose. *Id.* at 14–17.

Fifth, the Court dismissed Plaintiffs' Louisiana redhibition claim because Hauck, the sole Louisiana plaintiff, made only conclusory allegations parroting the elements of a redhibition claim. *Id.* at 17–18.

Sixth, the Court dismissed Plaintiffs' California negligence claim for failure to adequately allege property damage. *Id.* at 18–20.

The Court gave Plaintiffs leave to amend the claims dismissed in the order. *Id.* at 20. The Court informed Plaintiffs that "failure to cure the deficiencies identified in this Order will result in dismissal with prejudice of the claims dismissed in this Order." *Id.*

On November 9, 2018, AMD filed a motion to stay discovery until Plaintiffs' pleadings survived a motion to dismiss under Federal Rule of Civil Procedure 12(b)(6). ECF No. 90. On November 14, 2018, the Court *sua sponte* stayed discovery pending the Court's ruling on AMD's instant motion to dismiss. ECF No. 93.

On December 6, 2018, Plaintiffs filed the second consolidated amended complaint ("SCAC"). ECF No. 95. The SCAC spans 121 pages and includes 24 causes of action. *Id.* Plaintiffs no longer bring a cause of action for negligence, one of the eight causes of action the parties originally elected to litigate through summary judgment. *Id.* at ¶ 569. Accordingly, the parties are now litigating seven causes of action through summary judgment. As explained in more detail below, the SCAC refers generally to the Spectre mis-speculation vulnerability that Google Project Zero disclosed to AMD in June 2017 and that journalists disclosed to the public beginning on January 2, 2018, but conspicuously avoids using the term "Spectre."

On January 3, 2019, AMD filed a motion to dismiss the SCAC. ECF No. 97 ("Mot."). AMD moves to dismiss the remaining seven causes of action that the parties are litigating to summary judgment: (1) Count III for unfair practices under the UCL; (2) Count V for fraud by omission; (3) Count VII for breach of express warranty; (4) Count VIII for breach of the implied warranty of merchantability; (5) Count XI for violation of FDUTPA; (6) Count XVII for

redhibition; and (7) Count XIX for violation of the MCPA.

On January 24, 2019, Plaintiffs filed their opposition. ECF No. 101 ("Opp."). On February 7, 2019, AMD replied. ECF No. 104 ("Reply").

AMD also asks the Court to take judicial notice of nine documents. ECF No. 98. Plaintiffs oppose AMD's request in part, and themselves ask the Court to take judicial notice of one document. ECF No. 102. In its ruling on the motion to dismiss, the Court has not relied upon any of the documents in either AMD's request for judicial notice or Plaintiffs' request for judicial notice. Therefore, the Court denies as moot AMD's and Plaintiffs' requests for judicial notice.

II. LEGAL STANDARD

A. Motion to Dismiss Under Federal Rule of Civil Procedure 12(b)(6)

Rule 8(a)(2) of the Federal Rules of Civil Procedure requires a complaint to include "a short and plain statement of the claim showing that the pleader is entitled to relief." A complaint that fails to meet this standard may be dismissed pursuant to Federal Rule of Civil Procedure 12(b)(6). The U.S. Supreme Court has held that Rule 8(a) requires a plaintiff to plead "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). "The plausibility standard is not akin to a probability requirement, but it asks for more than a sheer possibility that a defendant has acted unlawfully." *Id.* (internal quotation marks omitted). For purposes of ruling on a Rule 12(b)(6) motion, the Court "accept[s] factual allegations in the complaint as true and construe[s] the pleadings in the light most favorable to the nonmoving party." *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008).

The Court, however, need not accept as true allegations contradicted by judicially noticeable facts, *see Schwarz v. United States*, 234 F.3d 428, 435 (9th Cir. 2000), and it "may look beyond the plaintiff's complaint to matters of public record" without converting the Rule 12(b)(6)

motion into a motion for summary judgment, *Shaw v. Hahn*, 56 F.3d 1128, 1129 n.1 (9th Cir. 1995). Nor must the Court "assume the truth of legal conclusions merely because they are cast in the form of factual allegations." *Fayer v. Vaughn*, 649 F.3d 1061, 1064 (9th Cir. 2011) (per curiam) (internal quotation marks omitted). Mere "conclusory allegations of law and unwarranted inferences are insufficient to defeat a motion to dismiss." *Adams v. Johnson*, 355 F.3d 1179, 1183 (9th Cir. 2004).

B. Motion to Dismiss Under Federal Rule of Civil Procedure 9(b)

Claims sounding in fraud are subject to the heightened pleading requirements of Federal Rule of Civil Procedure 9(b). *Bly-Magee v. California*, 236 F.3d 1014, 1018 (9th Cir. 2001). Under the federal rules, a plaintiff alleging fraud "must state with particularity the circumstances constituting fraud." Fed. R. Civ. P. 9(b). To satisfy this standard, the allegations must be "specific enough to give defendants notice of the particular misconduct which is alleged to constitute the fraud charged so that they can defend against the charge and not just deny that they have done anything wrong." *Semegen v. Weidner*, 780 F.2d 727, 731 (9th Cir. 1985). Thus, claims sounding in fraud must allege "an account of the time, place, and specific content of the false representations as well as the identities of the parties to the misrepresentations." *Swartz v. KPMG LLP*, 476 F.3d 756, 764 (9th Cir. 2007). In other words, "[a]verments of fraud must be accompanied by 'the who, what, when, where, and how' of the misconduct charged." *Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1106 (9th Cir. 2003) (citation omitted). The plaintiff must also plead facts explaining why the statement was false when it was made. *See In re GlenFed, Inc. Sec. Litig.*, 42 F.3d 1541, 1549 (9th Cir. 1994) (en banc), *superseded by statute on other grounds as stated in Marksman Partners, L.P. v. Chantal Pharm. Corp.*, 927 F. Supp. 1297 (C.D. Cal. 1996).

"When an entire complaint … is grounded in fraud and its allegations fail to satisfy the heightened pleading requirements of Rule 9(b), a district court may dismiss the complaint . . . ." *Vess*, 317 F.3d at 1107. The Ninth Circuit has recognized that "it is established law in this and

other circuits that such dismissals are appropriate," even though "there is no explicit basis in the text of the federal rules for the dismissal of a complaint for failure to satisfy 9(b)." *Id.* A motion to dismiss a complaint "under Rule 9(b) for failure to plead with particularity is the functional equivalent of a motion to dismiss under Rule 12(b)(6) for failure to state a claim." *Id.*

C. Leave to Amend

If the Court determines that a complaint should be dismissed, it must then decide whether to grant leave to amend. Under Rule 15(a) of the Federal Rules of Civil Procedure, leave to amend "shall be freely given when justice so requires," bearing in mind "the underlying purpose of Rule 15 to facilitate decisions on the merits, rather than on the pleadings or technicalities." *Lopez v. Smith*, 203 F.3d 1122, 1127 (9th Cir. 2000) (en banc) (alterations and internal quotation marks omitted). When dismissing a complaint for failure to state a claim, "a district court should grant leave to amend even if no request to amend the pleading was made, unless it determines that the pleading could not possibly be cured by the allegation of other facts." *Id.* at 1130 (internal quotation marks omitted). Accordingly, leave to amend generally shall be denied only if allowing amendment would unduly prejudice the opposing party, cause undue delay, or be futile, or if the moving party has acted in bad faith. *Leadsinger, Inc. v. BMG Music Publ'g*, 512 F.3d 522, 532 (9th Cir. 2008).

III. DISCUSSION

AMD's motion to dismiss challenges the following claims in Plaintiffs' SCAC: (1) Count III for unfair practices under California's UCL; (2) Count V for fraud by omission; (3) Count VII for breach of express warranty; (4) Count VIII for breach of the implied warranty of merchantability; (5) Count XI for violation of FDUTPA; (6) Count XVII for redhibition; and (7) Count XIX for violation of the MCPA. At a high level, the claims fall into three buckets: fraud claims, warranty claims, and the Louisiana redhibition claim.

A. Plaintiffs' Failure to Define the Defect

The Court first discusses Plaintiffs' continued failure to define "the Defect." The Court's

previous order dismissing Plaintiffs' CAC explained that "[g]iven Plaintiffs' vague and inconsistent definitions of Defect, AMD can hardly be expected to know exactly what the contents of its alleged misrepresentations are." MTD Order at 9.

Plaintiffs' CAC defined the Defect as "20 years [of] serious security vulnerabilities," CAC at ¶ 1, but the CAC also referred to Spectre—the mis-speculation vulnerability that Google Project Zero disclosed to AMD in June 2017 and that journalists disclosed to the public beginning on January 2, 2018—as the Defect. For example, Plaintiffs alleged that "Defendant knowingly sold or leased a defective product without informing customers about the Spectre Defect." *Id.* at ¶ 484. Plaintiffs described Spectre as: "To exploit a high-speed CPU's speculative execution capability, an attacker writes a piece of malicious code that causes the processor to 'mispredict' the result of a branch instruction, incuding the CPU to speculatively execute instructions that it otherwise would not execute." *Id.* at ¶ 14. The CAC further alleged that, "It is these speculative instructions, executed on the mispredicted path, that leak the information that the attacker is then able to recover." *Id.*

Plaintiffs' CAC alleged that AMD became aware of Spectre on June 1, 2017 at the latest when Google Project Zero disclosed the vulnerability to AMD. *Id.* at ¶ 84. Plaintiffs claimed that had they known about Spectre, they would not have purchased the computers or chips or would have paid less for them. *Id.* at ¶¶ 21–26. Plaintiffs also claimed that third-party patches to fix Spectre—patches that AMD did not develop or release—significantly reduce processing speed. *Id.* at ¶ 19.

Then, in Plaintiffs' opposition to AMD's first motion to dismiss, Plaintiffs claimed that the Defect was not Spectre, but rather "the security vulnerabilities created by AMD's design." ECF No. 73 at 1. However, as the Court explained, "Plaintiffs fail[ed] to identify what security vulnerabilities affected AMD's processors for the last 20 years *other than Spectre* and fail[ed] to explain how AMD's design created those vulnerabilities." MTD Order at 9 (emphasis added). Plaintiffs could only "point to vague sweeping statements about industry research and general

knowledge garnered from conference and academic papers" about *potential* security vulnerabilities. *Id.* at 11. The Court granted Plaintiffs leave to amend their pleadings, but Plaintiffs have again failed to define the Defect in the SCAC.

Although Plaintiffs do not mention Spectre in their 121-page SCAC, the SCAC's description of the mis-speculation vulnerability mirrors the CAC's description of Spectre. The SCAC alleges that in June 2017, a third party, Google Project Zero, informed AMD "of several new methods pursuant to which attackers could exploit the Defect," SCAC at ¶ 163, and that beginning on January 2, 2018, journalists published articles that disclosed the vulnerability to the public. *Id.* at ¶¶ 160–61. Plaintiffs state, "Mis-speculation is a normal function of the CPU when its branch predictor has incorrectly 'guessed' the next instructions the CPU needs to execute and the CPU speculatively executes instructions down the mispredicted path." *Id.* at ¶ 113. Plaintiffs describe the vulnerability as: "both the speculative execution process and the branch predictor in AMD's CPUs can be coerced by an attacker to speculatively execute unnecessary instructions hand-picked by the attacker, leading to intentional mis-speculation." *Id.* at ¶¶ 113, 163. *Id.* An attacker can use such intentional mis-speculation to reveal a CPU user's personal information. *Id.* at ¶¶ 113–14. This mirrors Plaintiffs' description of Spectre in the CAC: "To exploit a high-speed CPU's speculative execution capability, an attacker writes a piece of malicious code that causes the processor to 'mispredict' the result of a branch instruction, inducing the CPU to speculatively execute instructions that it otherwise would not execute." CAC ¶ 14

Instead of explicitly relying on Spectre, as Plaintiffs' CAC did, Plaintiffs' SCAC defines the Defect even more vaguely. Plaintiffs' SCAC identifies the Defect as "AMD's use of branch prediction, speculative execution, and caches in its CPU design," which Plaintiffs allege "created an inherent defect in the CPU that compromised consumers' most sensitive information." SCAC at ¶ 107.

Plaintiffs' opposition to the instant motion to dismiss makes contradictory statements. First, Plaintiffs concede that the SCAC is describing Spectre, which is the "set of exploits

publicized in early January 2018." Opp. at 2, 18. Second, the opposition tries to provide yet another vague definition of the Defect without mentioning Spectre: "key CPU microarchitectural components—branch prediction, speculative execution, and caches—caused consumers' sensitive data to be left unsecured by AMD." Opp. at 7.

Plaintiffs have omitted any specific references to Spectre because Google Project Zero disclosed Spectre's existence to AMD in June 2017, after all Plaintiffs except for Caskey-Medina purchased their AMD processors. Therefore, if Spectre is the vulnerability, Plaintiffs cannot allege that AMD knew about the vulnerability before Plaintiffs purchased their processors between July 2013 and November 2016, and thus cannot allege omission claims. *See Williams v. Yamaha Motor Co.*, 851 F.3d 1015, 1025 (9th Cir. 2017) ("[A] party must allege . . . that the manufacturer knew of the defect at the time a sale was made.") (citing *Apodaca v. Whirlpool Corp.*, 2013 WL 6477821, at *9 (C.D. Cal. Nov. 8, 2013)).

Further, if Spectre is the vulnerability, journalists disclosed Spectre to the public on January 2, 2018, before Caskey-Medina purchased his AMD processor on January 6, 2018, and Caskey-Medina thus cannot allege that he failed to receive the benefit of his bargain. *See also* Opp. at 15 n.17 (conceding that Spectre was "made public and discussed extensively in the press" before Caskey-Medina purchased his processor).

As a result, Plaintiffs' SCAC and opposition to the instant motion to dismiss vaguely define the Defect and claim that the Defect encompasses 20 years of AMD designs in order to attempt to allege that AMD knew about security vulnerabilities before Plaintiffs purchased their processors. *See* SCAC at ¶ 107 (alleging that AMD's use of branch prediction, speculative execution, and caches in its CPU designs has delivered dramatic performance improvements since 1995," but "created an inherent defect in the CPU that compromised consumers' most sensitive information"). However, as before, Plaintiffs fail to identify what security vulnerabilities affected AMD's processors *other than Spectre* and fail to explain how AMD's designs created those vulnerabilities.

That is the tension inherent in Plaintiffs' SCAC: Plaintiffs must rely on Spectre because it is the only identified security vulnerability affecting AMD's processors, but Plaintiffs must also disclaim any reliance on Spectre because Caskey-Medina purchased his AMD processor with knowledge of Spectre (and thus cannot claim that he failed to receive the benefit of his bargain) and because Google Project Zero disclosed Spectre to AMD after the remaining Plaintiffs purchased their AMD processors and thus Plaintiffs cannot allege viable omission claims.

That tension is also evident in Plaintiffs' allegations regarding standing, which rely exclusively on Spectre-related events, and not on any other security vulnerabilities. Thus, before addressing the problems with Plaintiffs' individual claims, the Court discusses AMD's challenge to Plaintiffs' standing.

B. Standing

AMD contends that Plaintiffs lack standing under Article III of the United States Constitution. AMD did not raise a standing argument in its first motion to dismiss, *see generally* ECF No. 64, and thus the Court has not previously addressed this issue. The Court concludes that Plaintiffs have standing to sue based on the SCAC's Spectre allegations.

"[S]tanding is an essential and unchanging part of the case-or-controversy requirement of Article III." *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992). Article III standing requires that (1) the plaintiffs suffered an injury in fact, i.e., "an invasion of a legally protected interest which is (a) concrete and particularized, and (b) actual or imminent, not conjectural or hypothetical"; (2) the injury is "'fairly traceable' to the challenged conduct"; and (3) the injury is "likely" to be "redressed by a favorable decision." *Id.* at 560–61. "[A]t the motion to dismiss stage, the plaintiff must clearly . . . allege facts demonstrating each element." *Spokeo v. Robins*, 136 S. Ct. 1540, 1547 (2016) (citation and internal quotation marks omitted) (ellipses in original). In class actions, "standing is satisfied if at least one named plaintiff meets the requirements." *Bates v. United Parcel Serv., Inc.*, 511 F.3d 974, 985 (9th Cir. 2007) (citation omitted).

AMD contends that Plaintiffs have not adequately alleged that Plaintiffs suffered an injury-

in-fact because any risk that a security vulnerability may lead to unauthorized access of Plaintiffs' data is speculative. As the U.S. Supreme Court has explained, "threatened injury must be certainly impending to constitute injury in fact." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409 (2013) (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990)). Plaintiffs need not demonstrate "that it is literally certain that the harms they identify will come about," as standing may be "based on a 'substantial risk' that the harm will occur." *Id.* at 414 n.5 (citation omitted). However, "allegations of possible future injury" based on "a highly attenuated chain of possibilities" do not suffice. *Id.* at 409–10 (alteration and citation omitted).

In the data breach context, the Ninth Circuit has held that where plaintiffs "have alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal information," the injury-in-fact requirement is satisfied. *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010). However, the Ninth Circuit also observed in *Krottner* that "if no laptop had been stolen, and Plaintiffs had sued based on the *risk* that it would be stolen at some point in the future[,] we would find the threat far less credible." *Id.* (emphasis added). In *In re Zappos.com, Inc.*, the Ninth Circuit followed *Krottner*'s reasoning and held that plaintiffs possessed Article III standing where attackers had accessed the plaintiffs' confidential information but had not yet misused the information. 888 F.3d 1020, 1027–28 (9th Cir. 2018), *cert. denied*, __ S. Ct. __, 2019 WL 1318579 (Mar. 25, 2019). Such a breach left the plaintiffs at an imminent, "substantial risk" of identity theft or identity fraud. *Id.* at 1028.

By contrast, in the instant case, no Plaintiff alleges that any attacker ever accessed any named Plaintiff's confidential information (or any AMD processor owner's confidential information) as a result of any security vulnerability, whether Spectre or some other unidentified vulnerability. *See also In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 2017 WL 3727318, at *12–13 (N.D. Cal. Aug. 30, 2017) (concluding plaintiffs alleged an Article III injury where hackers actually accessed the plaintiffs' private information and private information was being sold on dark web).

Thus, Plaintiffs argue in their opposition that "Plaintiffs' standing is not based on a risk of future harm (*e.g.*, a data breach)." Opp. at 10. Rather, the SCAC alleges that the named plaintiffs experienced slowdowns in clock speed after installing patches—patches that AMD did not develop or release—to mitigate the security vulnerability that journalists disclosed to the public beginning on January 2, 2018. Plaintiffs' opposition to the instant motion to dismiss identifies the vulnerability that journalists disclosed to the public in January 2018 as Spectre, even though Plaintiffs do not mention the term "Spectre" in the SCAC. Opp. at 2 (referring to Spectre as "the set of exploits publicized in early January 2018"). For example, the SCAC alleges that after learning about Spectre, Pollack installed a patch released by a third party, and that his processor "crash[ed] more often and need[ed] more frequent reboots"—especially when Pollack played computer games. SCAC ¶ 26. In the SCAC, Hauck alleges that once she installed a Spectre patch released by a third party, "her computer frequently crashed, sometimes several times per day." *Id.* at ¶ 10. All named Plaintiffs allege in the SCAC that had they been aware of Spectre and that efforts to mitigate the vulnerability would impede the processors' performance, they "would not have purchased the computer, or paid substantially less for the computer [or processor]." *Id.* at ¶¶ 11, 15, 19, 23, 28, 33.

Under Ninth Circuit precedent, Plaintiffs' allegations are sufficient to state an injury-in-fact. The Ninth Circuit has repeatedly held that overpayment is a cognizable Article III injury. *See Mazza v. Am. Honda Motor Co.*, 666 F.3d 581, 595 (9th Cir. 2012) (holding that plaintiffs alleged an injury where "class members paid more for [a product] that they otherwise would have paid, or bought it when they otherwise would not have done so"); *see also Hinojos v. Kohl's Corp.*, 718 F.3d 1098, 1104 n. 3 (9th Cir. 2013) (explaining that there is "no difficulty . . . regarding Article III injury" when plaintiffs allege that they either overpaid for a product or would not have purchased the product); *In re Yahoo*, 2017 WL 3727318, at *17 (finding that plaintiffs' allegations of benefit of the bargain damages were sufficient to allege an Article III injury).

While some courts have rejected conclusory overpayment allegations, Plaintiffs here have

alleged that their processors experienced performance slowdowns after Plaintiffs installed patches developed to address Spectre. Plaintiffs do not allege that AMD developed or released any patches. Pollack "stopped using his computer for gaming and later ceased to use the processor altogether." SCAC at ¶ 27; *see also In re Volkswagen "Clean Diesel" Mktg., Sales Practices & Prods. Liability Litig.*, 349 F. Supp. 3d 881, 893 (N.D. Cal. 2018) (explaining that "[u]nderlying these no-injury defect cases is a critical eye toward allegations of overpayment for [products] that essentially work as advertised"). Therefore, Plaintiffs have adequately alleged an injury.

AMD contends that Plaintiffs have not alleged a causal connection between any security vulnerability and the performance of Plaintiffs' devices. However, "[a] causal chain does not fail simply because it has several links, provided those links are not hypothetical or tenuous and remain plausible." *Maya v. Centex Corp.*, 658 F.3d 1060, 1070 (9th Cir. 2011) (internal quotation marks and citations omitted). Simply put, the line of causation between a defendant's actions and a plaintiff's harm must not be attenuated. *Id.* (citing *Allen v. Wright*, 468 U.S. 737, 757 (1984)). Plaintiffs' SCAC alleges that after Plaintiffs installed patches that third parties developed to mitigate the Spectre vulnerability that journalists disclosed to the public beginning on January 2, 2018, Plaintiffs' processors experienced reduced performance, which raises the inference that the patches caused the reduced performance. *See* SCAC ¶¶ 10, 27.

Two recent cases decided in this district further demonstrate why Plaintiffs have adequately alleged that their injuries are "fairly traceable" to AMD's conduct. *Lujan*, 504 U.S. at 560. In *In re Apple Processor Litigation*, 2019 WL 79035 (N.D. Cal. Jan. 2, 2019), which Plaintiffs cite and which involved allegations against Apple based on the Spectre vulnerability, the district court held that the plaintiffs failed to establish standing because none of the named plaintiffs had "personally experienced a degradation of performance of their iDevices." *Id.* at *3. Further, tests on Apple processors failed to support an inference of reduced performance. *Id.* at *4. Similarly, in *Beyer v. Symantec Corp.*, 2019 WL 935135 (N.D. Cal. Feb. 26, 2019), the district court concluded that plaintiffs lacked standing where plaintiffs did not allege that they

personally experienced performance problems after installing allegedly deficient antivirus software. *Id.* at *4.

By contrast, all Plaintiffs in the instant case have alleged that they personally experienced decreased performance of their processors after installing patches that third parties—not AMD—released to mitigate the Spectre vulnerability. Accordingly, the Court concludes that Plaintiffs have adequately alleged an injury-in-fact that is fairly traceable to AMD's conduct. Of course, as discussed above, this conclusion—that only Spectre-related events provide Plaintiffs standing—demonstrates the tension in Plaintiffs' simultaneous attempt to disclaim Spectre and broadly define the Defect as 20 years of unspecified security vulnerabilities.

Further, it is a separate question whether Plaintiffs have adequately alleged facts to state a plausible claim for relief, and whether Plaintiffs have alleged those facts with particularity. *See Phillips v. Apple, Inc.*, 2016 WL 5846992, at *2 (N.D. Cal. Oct. 6, 2016) (distinguishing the "modest" showing required for Article III standing from the question of "whether Plaintiffs have stated a plausible claim for relief").

C. Fraud Claims

The Court next addresses Plaintiffs' consumer fraud claims. Plaintiffs assert MCPA, FDUTPA, and California fraud by omission claims. As explained above, Plaintiffs' SCAC suffers from an inherent tension: Plaintiffs must rely on Spectre because it is the only identified security vulnerability affecting AMD's processors, but Plaintiffs must also disclaim any reliance on Spectre because Caskey-Medina purchased his AMD processor with knowledge of Spectre (and thus cannot claim that he failed to receive the benefit of his bargain) and because AMD learned about Spectre after the remaining Plaintiffs purchased their AMD processors and thus Plaintiffs cannot allege viable omission claims.

1. Omission Claims

Fraud claims based on omissions are cognizable under both FDUTPA and MCPA. *See Keegan v. Am. Honda Motor Co., Inc.*, 838 F. Supp. 2d 929, 959 (C.D. Cal. 2012) (holding that

Florida courts construe FDUTPA "to permit claims based on omissions alone") (citing *Millennium Commc'ns & Fulfillment, Inc. v. Office of the Att'y Gen.*, 761 So.2d 1256, 1263 (Fla. App. 2000)); *Aspinall v. Philip Morris Cos., Inc.*, 813 N.E.2d 476, 487–88 (Mass. 2004) (holding that a "material, knowing, and willful nondisclosure" violates the MCPA).

Further, the parties do not dispute that Rule 9(b)'s heightened particularity standard applies to MCPA fraud claims. *See Watkins v. Omni Life Sci., Inc.*, 692 F. Supp. 2d 170, 177 (D. Mass. 2010) (applying Rule 9(b) to MCPA fraud claims).

As for FDUTPA, there is a split of authority among Florida courts as to whether Rule 9(b) applies to FDUTPA claims. *State Farm Mut. Auto. Ins. Co. v. Performance Orthopaedics & Neurosurgery, LLC*, 278 F. Supp. 3d 1307, 1328 (S.D. Fla. 2017). Nevertheless, this Court applies Ninth Circuit law, which requires the application of Rule 9(b)'s heightened pleading standards to entire claims that sound in fraud even if fraud is not an element of the claim. *Vess*, 317 F.3d at 1103–04 (holding that where a plaintiff's claim sounds in fraud, "the pleading of that claim as a whole" must satisfy Rule 9(b)). Previously, the Court applied Rule 9(b)'s heightened pleading standards to Plaintiffs' FDUTPA claim because the FDUTPA claim alleged that AMD engaged in fraud. MTD Order at 8. Plaintiffs' FDUTPA claim in the SCAC again sounds in fraud. SCAC at ¶ 362 ("Defendant violated FDUPTA by . . . fraudulently concealing the existence of the Defect in its processors."). Therefore, the Court finds that Rule 9(b) applies to Plaintiffs' FDUTPA claim.

Under Ninth Circuit precedent, "[a]llegations of fraud must be specific enough to give defendants notice of the particular misconduct which is alleged to constitute the fraud charged . . . ." *Bly-Magee*, 236 F.3d at 1019. Moreover, the Ninth Circuit has held that Rule 9(b) applies to fraud claims based on omission. *See Kearns*, 567 F.3d at 1126 (holding that omissions claims are fraud claims that must meet Rule 9(b)'s heightened pleading analysis). Thus, to satisfy Rule 9(b), Plaintiffs must "provide [AMD] with the 'who, what, when, and where' of [AMD's] allegedly fraudulent omissions." *Davidson v. Apple, Inc.*, 2017 WL 3149305, at *13 (N.D. Cal. July 25,

2017) (citing *Kearns*, 567 F.3d at 1127).

To state omission claims, Plaintiffs must also allege that AMD had actual knowledge of the information that AMD allegedly omitted. Under California law, a manufacturer must have known of the defect at the time of sale for a plaintiff to state a claim for fraud by omission against the manufacturer. *Williams*, 851 F.3d at 1025 ("[A] party must allege . . . that the manufacturer knew of the defect at the time a sale was made."). The same is true under FDUTPA. *See Matthews v. Am. Honda*, 2012 WL 2520675, at *3 (S.D. Fla. Jun. 6, 2012) ("Florida courts have recognized that a FDUTPA claim is stated where defendant knowingly fails to disclose a material defect."). Although Plaintiffs contend that the MCPA contains no "knowledge" requirement, the Massachusetts Supreme Court has squarely held that under the MCPA, "[t]here is no liability for failing to disclose what a person does not know." *Underwood v. Risman*, 605 N.E.2d 832, 835 (Mass. 1993). Other district courts in this district, in applying the MCPA, have inquired whether the defendant "knew about the defect at the time of each sale." *See, e.g.*, *In re Myford Touch Consumer Litig.*, 2018 WL 3646895, at *3 (N.D. Cal. Aug. 1, 2018).

Moreover, a plaintiff may not state an omission claim with allegations that a defendant *should have* known about a defect from general knowledge. *Morris v. BMW of N. Am., LLC*, 2007 WL 3342612, at *6 (N.D. Cal. Nov. 7, 2007) (holding that allegations that the defendant "should have known" of a defect were insufficient to state a fraud by omission claim, and that the plaintiff must instead allege that the defendant had "actual knowledge" of the defect).

The Court previously dismissed Plaintiffs' omission claim because "Plaintiffs [did] not actually allege [AMD's] actual knowledge of the Defect prior to when Plaintiffs purchased the AMD processors or computers." MTD Order at 11. Plaintiffs could only identify "vague, sweeping statements about industry research and general knowledge garnered from conferences and academic papers of the Defect's potential to exploit processors and gather confidential information." *Id.* Plaintiffs alleged only that AMD knew of a security vulnerability in June 2017, when Google Project Zero disclosed Spectre to AMD. *Id.* at 10–11.

Like the CAC, the SCAC describes only a series of potential security vulnerabilities affecting CPUs in general or affecting non-AMD processors. *See, e.g.*, *id.* at ¶ 133 (describing exploit that "could" affect an *Intel* processor); ¶ 136 (researcher stating generally that companies should identify microarchitectural attacks); ¶ 138 (explaining that side-channel attacks can "exploit[] the natural function of a CPU"). Plaintiffs' vague allegations about general knowledge are insufficient to allege that AMD knew of any specific security vulnerability affecting AMD processors, and fail to give AMD "notice of the particular misconduct of the fraud charged so that they can defend against the charge." *Semegen*, 780 F.2d at 731; *see also Morris*, 2007 WL 3342612, at *6 (allegations that a defendant "should have known" of defects are insufficient to state an omission claim).

As explained above, Plaintiffs' SCAC defines the Defect vaguely and without mentioning Spectre. Plaintiffs' SCAC identifies the Defect as "AMD's use of branch prediction, speculative execution, and caches in its CPU design," which Plaintiffs allege "created an inherent defect in the CPU that compromised consumers' most sensitive information." SCAC at ¶ 107. Plaintiffs' opposition to the instant motion to dismiss makes contradictory statements. First, Plaintiffs concede that the SCAC is describing Spectre, which is "the set of exploits publicized in early January 2018." Opp. at 2, 18. Second, the opposition tries to provide yet another vague definition of the Defect without mentioning Spectre: "key CPU microarchitectural components—branch prediction, speculative execution, and caches—caused consumers' sensitive data to be left unsecured by AMD." Opp. at 7. Plaintiffs' vague allegation that AMD's CPUs are themselves the Defect does not provide AMD notice of any particular security vulnerability in any particular AMD processor. *See Davidson v. Apple, Inc.*, 2017 WL 976408, at *10 (N.D. Cal. Mar. 14, 2017) (dismissing omission allegations that were "too vague" to advise the defendants of what defendants failed to disclose).

Plaintiffs have omitted any specific references to Spectre because Google Project Zero disclosed Spectre to AMD in June 2017, after all Plaintiffs except for Caskey-Medina purchased

their AMD processors. Further, if Spectre is the vulnerability, Plaintiffs cannot allege that AMD knew about the vulnerability before Plaintiffs purchased their processors between July 2013 and November 2016, and thus cannot allege omission claims. *See Williams*, 851 F.3d at 1025 ("[A] party must allege . . . that the manufacturer knew of the defect at the time a sale was made.").

As for Caskey-Medina, journalists disclosed Spectre to the public on January 2, 2018, before Caskey-Medina purchased his AMD processor on January 6, 2018. Thus, Caskey-Medina cannot allege that he failed to receive the benefit of his bargain. In fact, Caskey-Medina does not allege that he was unaware of Spectre when he purchased his processor, *see* SCAC at ¶¶ 29–33, and Plaintiffs concede that Spectre "was made public and discussed extensively in the press" before Caskey-Medina purchased his processor on January 6, 2018. Opp. at 15 n.17. Caskey-Medina cannot plausibly allege that AMD is liable for failing to disclose to Caskey-Medina information that was already public. *See Carlson v. The Gillette Co.*, 2015 WL 6453147, at *6 (D. Mass. Oct. 23, 2015) (holding that to violate the MCPA, a nondisclosure must be "likely to mislead a reasonable consumer").

As a result, Plaintiffs' SCAC and opposition to the instant motion to dismiss vaguely define the Defect and claim that the Defect encompasses 20 years of AMD designs in order to attempt to allege that AMD knew about security vulnerabilities before all Plaintiffs except for Caskey-Medina purchased their processors. *See* SCAC at ¶ 107 (alleging that AMD's use of branch prediction, speculative execution, and caches in its CPU designs has delivered dramatic performance improvements since 1995," but "created an inherent defect in the CPU that compromised consumers' most sensitive information"). However, Plaintiffs again fail to identify what security vulnerabilities affected AMD's processors *other than Spectre* and fail to explain how AMD's designs created those vulnerabilities. Plaintiffs' allegations are insufficient to show that AMD knew of any security vulnerability affecting AMD processors before June 2017, when Google Project Zero disclosed Spectre to AMD. SCAC at ¶ 163.

Therefore, Plaintiffs have failed to adequately plead fraudulent omission claims under

California law, the MCPA, or FDUTPA. The Court finds that granting Plaintiffs leave to amend their omission claims would be futile and unduly prejudicial to AMD. *Leadsinger, Inc.*, 512 F.3d at 532. In its prior Order dismissing Plaintiffs' CAC, the Court dismissed Plaintiffs' omission claims because Plaintiffs failed to define the Defect with any particularity and failed to allege AMD's pre-purchase knowledge of the Defect. MTD Order at 11–12. The Court warned that "failure to cure the deficiencies identified in this Order will result in dismissal with prejudice." *Id.* at 20. Plaintiffs failed to cure the deficiencies, and the Court is dismissing Plaintiffs' omission claims in the SCAC for the same reasons that the Court dismissed Plaintiffs' omission claims in the CAC. If anything, the SCAC defines the Defect even more vaguely than the CAC, and again relies on allegations of general industry knowledge to attempt to show AMD's pre-purchase knowledge of the Defect. Because any amendment would be futile, and it would be unduly prejudicial to AMD to litigate a third motion to dismiss regarding the same deficiencies—especially given the voluminous claims in this case—the Court DENIES Plaintiffs leave to amend their fraudulent omissions claims under California law, the MCPA, and FDUTPA.

2. Affirmative Misrepresentations under MCPA and FDUTPA

Plaintiffs also bring affirmative misrepresentation claims under MCPA and FDUTPA. The Court previously dismissed Plaintiffs' affirmative misrepresentation claims because Plaintiffs failed to plead "why [AMD's] representations of clock speed were false." MTD Order at 9.

In the SCAC, Plaintiffs again fail to allege that AMD made any false representations. To satisfy Rule 9(b), a plaintiff must allege why a statement was "untrue or misleading *when made*." *In re Glenfed*, 42 F.3d at 1549 (emphasis in original). Claims sounding in fraud must also allege "an account of the time, place, and specific content of the false representations as well as the identities of the parties to the misrepresentations." *Swartz*, 476 F.3d at 764.

Plaintiffs contend that AMD's "representations of clock speed are misleading because its CPUs are incapable of reaching the advertised clock speeds without sacrificing security." Opp. at 13. However, Plaintiffs fail to point to any AMD representations about *security*. The fact that

AMD's clock speeds allegedly come hand-in-hand with a security vulnerability does not render AMD's representations about clock speed false. Plaintiffs' SCAC even acknowledges that AMD's representations about clock speed are *true*. *See id.* at ¶ 61 (AMD CPUs reached their "advertised speed" due to the design decisions that Plaintiffs allege constitute the Defect). As before, "Plaintiffs never identify any basis (reasonable or otherwise) for their supposed understanding that the clock speed also constituted a 'promise' that the processors would be immune to security threats." MTD Order at 10.

Alternatively, Plaintiffs contend that AMD's clock speed representations were false when made because Plaintiffs later installed third-party patches—patches that AMD did not release or develop—that slowed the processors' clock speed. Opp. at 14. However, Plaintiffs are unable to identify any AMD representations about processor clock speed with any installed patch—much less third-party patches. Plaintiffs can identify only representations about an AMD processor's clock speed as sold. *See* SCAC ¶ 17 (alleging only that the "AMD processor's specifications, including its clock speed or frequently, were prominently displayed on the box and on the receipt"). Again, Plaintiffs' SCAC acknowledges that AMD's representations about clock speed are *true*. *See id.* at ¶ 61.

Therefore, Plaintiffs have not alleged that AMD made any representations that were "actually false" when made, *Davis v. HSBC Bank Nev., N.A.*, 691 F.3d 1152, 1162 (9th Cir. 2012), and have not stated a claim based on any affirmative misrepresentations.

The Court finds that granting Plaintiffs leave to amend their affirmative misrepresentation claims under the MCPA and FDUTPA would be futile and unduly prejudicial to AMD. *Leadsinger, Inc.*, 512 F.3d at 532. In its prior Order dismissing Plaintiffs' CAC, the Court dismissed Plaintiffs' fraud claims because Plaintiffs failed to define the Defect with particularity and failed to plead facts explaining AMD's representations about clock speed were false. MTD Order at 9. The Court warned that "failure to cure the deficiencies identified in this Order will result in dismissal with prejudice." *Id.* at 20. Plaintiffs failed to cure the deficiencies. As

explained above, the SCAC defines the Defect even more vaguely than the CAC. Further, Plaintiffs again fail to plead any facts suggesting that AMD's representations about clock speed were false when made. Because any amendment would be futile, and it would be unduly prejudicial to AMD to litigate a third motion to dismiss regarding the same deficiencies—especially given the voluminous claims in this case—the Court DENIES Plaintiffs leave to amend their affirmative misrepresentation claims under the MCPA and FDUTPA.

3. California UCL Unfair Prong Claim

The Court now turns to Plaintiffs' unfair prong UCL claim. The Court previously did not address this claim, as AMD previously mistakenly moved to dismiss only Plaintiffs' fraud prong UCL claim, which the parties had not elected to litigate at this stage. *See* MTD Order at 4 n.1. AMD now moves to dismiss Plaintiffs' unfair prong UCL claim, which the parties had previously elected to litigate. Mot. at 18.

The unfair prong of the UCL prohibits a business practice that "violates established public policy or if it is immoral, unethical, oppressive or unscrupulous and causes injury to consumers which outweighs its benefits." *McKell v. Wash. Mut., Inc.*, 142 Cal. App. 4th 1457, 1473 (2006). California law "is currently unsettled with regard to the standard applied to consumer claims under the unfair prong of the UCL." *Hadley v. Kellogg Sales Co.*, 243 F. Supp. 3d 1074, 1104 (N.D. Cal. 2017). Specifically, "[t]he California Supreme Court has rejected the traditional balancing test for UCL claims between business competitors and instead requires that claims under the unfair prong be 'tethered to some legislatively declared policy.'" *Id.* (quoting *Cel-Tech Commc'ns, Inc. v. L.A. Cellular Tel. Co.*, 20 Cal. 4th 163, 186 (1999)).

Nevertheless, regardless of the test, courts in this district have held that where the "plaintiffs' unfair prong claims overlap entirely with their claims of fraud," the plaintiffs' unfair prong claim cannot survive. *In re Actimmune Mktg. Litig.*, 2009 WL 3740648, at *14 (N.D. Cal. Nov. 6, 2009), *aff'd*, 464 F. App'x 651 (9th Cir. 2011); *see also Punian v. Gillette Co.*, 2016 WL 1029607, at *17 (N.D. Cal. Mar. 15, 2016) (holding unfair prong UCL cause of action does not

survive where the "cause of action under the unfair prong of the UCL overlaps entirely with [a plaintiff's] claims" alleging fraud that also do not survive); *see also Kearns*, 567 F.3d at 1127 (affirming dismissal of UCL claim grounded in fraud without further analysis after holding that plaintiff failed to adequately allege fraud).

Here, Plaintiffs' UCL unfair prong claim is premised on AMD's allegedly fraudulent omissions. *See* SCAC at ¶ 245 (alleging that AMD violated the UCL by "failing to disclose" the Defect). Therefore, Plaintiffs' unfair prong claim "overlaps entirely" with Plaintiffs' fraud claims, and must also fail. *Hadley*, 243 F. Supp. 3d at 1104. Regardless, the Ninth Circuit has squarely held that under the UCL, the "failure to disclose a . . . defect of which [a defendant] is not aware, does not constitute an unfair or fraudulent practice." *Wilson v. Hewlett-Packard Co.*, 668 F.3d 1136, 1145 n.5 (9th Cir. 2012) (citing *Daugherty v. Am. Honda Motor Co., Inc.*, 144 Cal. App. 4th 824, 838–39 (2006)). By any measure, Plaintiffs have failed to state a UCL unfair prong claim.

The Court finds that granting Plaintiffs leave to amend their UCL unfair prong claim would be futile and unduly prejudicial to AMD. *Leadsinger, Inc.*, 512 F.3d at 532. Plaintiffs' unfair prong claim is predicated on AMD's allegedly fraudulent omissions and, as explained above, Plaintiffs' SCAC suffers from the same deficiencies that the Court identified in Plaintiffs' CAC. Because any further amendment would be futile, and it would be unduly prejudicial to AMD to litigate a third motion to dismiss regarding the same deficiencies—especially given the voluminous claims in this case—the Court DENIES Plaintiffs leave to amend their UCL unfair prong claim.

C. Warranty Claims

The Court now turns to the breach of express warranty and implied warranty claims.

1. California Breach of Express Warranty

To prevail on a breach of express warranty claim under California law, Plaintiffs must prove that Defendants made "affirmations of fact or promise" or a "description of the goods" that became "part of the basis of the bargain." *Weinstat v. Dentsply Int'l, Inc.*, 180 Cal. App. 4th 1213,

1227 (2010); Cal. Comm. Code § 2313 (defining express warranty). In order to plead the exact terms of the warranty, the plaintiff must "identify a specific and unequivocal written statement about the product that constitutes an explicit guarantee." *Hadley*, 273 F. Supp. 3d at 1092 (internal quotations omitted); *see also Maneely v. Gen. Motors Corp.*, 108 F.3d 1176, 1181 (9th Cir. 1997) (same).

In its previous order, the Court dismissed Plaintiffs' warranty claim because Plaintiffs failed to plead the exact terms of the warranty and, even if a warranty was breached, failed to allege harm. MTD Order at 12. AMD contends that the SCAC suffers from the same deficiencies. In particular, AMD contends that Plaintiffs fail to identify any "specific and unequivocal written statement about the product that constitutes an explicit guarantee." Mot. at 20. In opposition, Plaintiffs are unable to quote any language from the SCAC alleging the terms of an express warranty. *See* Opp. at 18–19. AMD prevails here.

Plaintiffs argue only that "the performance specifications" are AMD's express warranty. *See* SCAC at ¶ 304 (alleging that AMD gave express warranties "regarding the security *and* processing speeds of the processors") (emphasis in original). However, Plaintiffs never cite the language of any CPU performance specifications or other written terms. All of the SCAC paragraphs Plaintiffs cite—SCAC ¶¶ 4-7, 11, 15, 19, 23, 28, 33, 61—refer only generally to "AMD's representations that the AMD processor would perform as advertised and was not defective." *Id.* at ¶ 33. Plaintiffs fail to cite any specific representation. The alleged terms of AMD's express warranty resemble the terms "said product was effective, proper and safe for its intended use and consumption," which this Court has held are too general to state express warranty claims. *Ferrari v. Nat. Partners, Inc.*, 2016 WL 4440242, at *10 (N.D. Cal. Aug. 23, 2016); *see also Maneely*, 108 F.3d at 1181 (holding that terms that "make no explicit guarantees" are not express warranties).

In sum, Plaintiffs' vague allegations fall far short of alleging the "exact terms of the warranty." *Williams v. Beechnut Nutrition Corp.*, 185 Cal. App. 3d 135, 142 (1986); *cf. Kellman*

v. Whole Foods Market, Inc., 313 F. Supp. 3d 1031, 1052 (N.D. Cal. 2018) (holding that plaintiff had adequately pled an express warranty claim based on a label representing that a product was "hypoallergenic"). Because the Court concludes that Plaintiffs have not alleged express warranty claims, the Court need not consider whether AMD's written warranty limitations disclaim any such express warranties. *See* Mot. at 22; Opp. at 20–22; *see also Davidson v. Apple, Inc.*, 2017 WL 976048, at *12–14 (N.D. Cal. Mar. 14, 2017) (considering unconscionability of warranty only after determining that warranty language was at issue).

Therefore, the Court dismisses Plaintiffs' breach of express warranty claim. The Court finds that granting Plaintiffs leave to amend their express warranty claim would be futile and unduly prejudicial to AMD. *Leadsinger, Inc.*, 512 F.3d at 532. In its prior Order dismissing Plaintiffs' CAC, the Court dismissed Plaintiffs' express warranty claims because Plaintiffs failed to allege the exact terms of an express warranty. MTD Order at 12. The Court warned that "failure to cure the deficiencies identified in this Order will result in dismissal with prejudice." *Id.* at 20. Plaintiffs have again failed to cite any terms of any express warranty, and have thus failed to cure the deficiencies the Court identified. Because any further amendment would be futile, and it would be unduly prejudicial to AMD to litigate a third motion to dismiss regarding the same deficiencies—especially given the voluminous claims in this case—the Court DENIES Plaintiffs leave to amend their breach of express warranty claim.

2. California Breach of Implied Warranty of Merchantability

The Court now turns to Plaintiffs' California claim for breach of the implied warranty of merchantability.[1]

Among other elements, the California implied warranty of merchantability requires that a product is "fit for the ordinary purpose for which such goods are used." *Mocek v. Alfa Leisure,*

[1] Plaintiffs previously raised a claim for breach of the implied warranty of fitness for a particular purpose, which the Court dismissed. MTD Order at 16–17. Plaintiffs represent that they "no longer allege a breach of implied warranty of fitness for a particular purpose under California law." Opp. at 9 n.10.

Inc., 114 Cal. App. 4th 402, 406 (2003); *see* Cal. Comm. Code § 2314(c). "[A] breach of the implied warranty [of merchantability] means the product did not possess even the most basic degree of fitness for ordinary use." *Mocek*, 114 Cal. App. 4th at 406. To state a claim that a product is unfit for its ordinary purpose, a plaintiff must allege that the defect seriously impacts the product's operability. *Troup v. Toyota Motor Corp.*, 545 F. App'x 668, 669 (9th Cir. 2013) (holding that a Prius vehicle was fit for its ordinary purpose because a defect did not "compromise the vehicle's safety, render it inoperable, or drastically reduce its mileage range"); *see also Birdsong v. Apple, Inc.*, 590 F.3d 955, 958 (9th Cir. 2009) (holding that the warranty of merchantability provides only that goods are of "a minimum level of quality") (internal quotation marks and citation omitted).

The Court previously dismissed Plaintiffs' implied warranty of merchantability claim because Plaintiffs' pleadings "contain[ed] no allegation that the basic functionality of the processors has been compromised by the Defect." MTD Order at 15. Specifically, Plaintiffs alleged only that patches decreased clock speed, and gave a "ballpark figure of five to 30 per cent slow down." *Id.* (quoting CAC at ¶ 93). Therefore, the Court concluded that the "AMD processors are certainly still operable even assuming they are patched, though the processors may be a little less efficient, much like the Priuses in *Troup*." *Id.*

The same holds true with Plaintiffs' SCAC. Plaintiffs now allege that Plaintiffs experienced slowdowns as a result of third-party patches, and that their AMD processors cannot "reach advertised specifications." Opp. at 22. Plaintiffs do not allege that AMD developed or released those patches. In addition, even where Plaintiffs have added more specific allegations about the performance slowdowns, Plaintiffs do not allege that the "basic functionality" of the processors has been compromised. For example, Plaintiff Garcia alleges that his computer ran "more slowly," but was still able to "perform[] graphics and video editing." SCAC at ¶ 18. Thus, even though Garcia "no longer uses the processor," Garcia does not allege that his processor is unusable—only that it is somewhat less efficient, and that he chose to stop using the processor.

Id. That is insufficient to state a claim for breach of the implied warranty of merchantability. *See Minkler v. Apple, Inc.*, 65 F. Supp. 3d 810, 819 (N.D. Cal. 2014) (holding that plaintiffs failed to state a claim absent allegations that product "failed to work at all or even that it failed to work a majority of the time"). Plaintiffs, by alleging only that their processors "run more slowly," have failed to allege that any AMD security vulnerability "drastically undermine[s] the ordinary operation" of the processors. *See Troup*, 545 F. App'x at 669.

Plaintiffs also argue that they can state a claim for breach of the implied warranty of merchantability because "ensuring the security of a user's information is a basic function of any CPU." Opp. at 8–9 (citing SCAC at ¶ 108). Plaintiffs argue, without citation, that "to compute securely" is "the most basic function of a processor." *Id.* at 22. Even accepting that conclusory premise as true, Plaintiffs fail to allege facts to support an implied warranty claim.

Courts have recognized that a breach of the implied warranty of merchantability claim may lie where a product *actively* interferes with a consumer's confidential information. *See In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1110 (N.D. Cal. 2018) (holding that plaintiffs stated implied warranty claim based on a mobile device defect that "actively intercepts and/or transmits personal communication data to third parties") (emphasis added); *see also In re Nexus 6P Prods. Liability Litig.*, 293 F. Supp. 3d 888, 925 (N.D. Cal. 2018) (plaintiffs' devices experienced "total failure" and plaintiffs "permanently [lost] access to any data stored" on the devices). Here, by contrast, Plaintiffs do not allege that *any* AMD processor owner—let alone any named Plaintiff—has lost any confidential information to Spectre or any other security vulnerability, or that a vulnerability "actively" interferes with Plaintiffs' information. Plaintiffs' vague allegations are insufficient to state a claim for breach of the implied warranty of merchantability.

The Court finds that granting Plaintiffs leave to amend their implied warranty claim would be futile and unduly prejudicial to AMD. *Leadsinger, Inc.*, 512 F.3d at 532. In its prior Order dismissing Plaintiffs' CAC, the Court dismissed Plaintiffs' implied warranty claim because Plaintiffs failed to allege that Plaintiffs' processors lacked basic functionality as processors. MTD

Order at 15. The Court warned that "failure to cure the deficiencies identified in this Order will result in dismissal with prejudice." *Id.* at 20. As explained above, Plaintiffs have again failed to plead facts sufficient to allege that Plaintiffs' processors lacked basic functionality. Because any further amendment would be futile, and it would be unduly prejudicial to AMD to litigate a third motion to dismiss regarding the same deficiencies—especially given the voluminous claims in this case—the Court DENIES Plaintiffs leave to amend their claim for breach of the implied warranty of merchantability.

D. Louisiana Redhibition Claim

The Court now turns to Plaintiffs' redhibition claim under Louisiana law. A redhibitory defect is one in which the defect "renders the thing useless, or its use so inconvenient that it must be presumed that a buyer would not have bought the thing had he known of the defect." La. Civ. Code art. 2520. Furthermore, a defect is redhibitory when the defect diminishes a product's usefulness or value so that a buyer would have bought it at a reduced price, or not at all. *Chevron USA, Inc. v. Aker Mar., Inc.*, 604 F.3d 888, 899 (5th Cir. 2010); *see also Becnel v. Mercedes-Benz USA, LLC*, 2014 WL 1918468, at *8 (E.D. La. May 13, 2014) (holding that plaintiff stated redhibition claim where he alleged that the defect rendered the product "unusable").

The Court previously dismissed Plaintiffs' redhibition claim because Hauck, the only Louisiana Plaintiff, "[did] not allege anything other than the elements of a rehibition claim." MTD Order at 18. Plaintiffs have amended the SCAC to allege that Hauck installed a third-party patch "that purportedly mitigated the risk to her sensitive information presented by the Defect." SCAC at ¶ 10. After Hauck installed the patch, her processor "no longer could achieve its advertised performance level, and her computer frequently crashed, sometimes several times per day." *Id.* at ¶ 11.

AMD contends that Plaintiffs' redhibition claim must again fail because Plaintiff Hauck fails to allege an adequate causal link between any security vulnerability and her processor's performance issues. Mot. at 24. Although Plaintiffs appear to concede AMD's point and do not

focus on the processor's performance, any patch-related performance issues are not a redhibitory defect because "[a] redhibitory defect must be latent and have existed at time of sale," and Plaintiffs all installed the patches post-sale. *Page v. Dunn*, 2017 WL 5599512, at *1, 3 (E.D. La. Nov. 21, 2017) (redhibition claim involving "toxic levels of mold" that allegedly made house uninhabitable). Regardless, Plaintiffs also do not allege that AMD developed or released any of the patches that any Plaintiff installed.

Plaintiffs contend that because security is so fundamental to a processor, Hauck's allegations that she would have paid less for the AMD processor if she had known about its security vulnerabilities, such as Spectre, are sufficient to state a redhibition claim. Opp. at 25. Yet Hauck again alleges no facts to support the conclusory, element-mirroring allegation that she would have paid less for the processor had she known of any security vulnerability. For example, Hauck does not allege that after journalists disclosed Spectre to the public in January 2018, the price of AMD processors or of other affected processors dropped or that AMD could not sell any processors. *See Justiss Oil Co., Inc. v. Oil Country Tubular Corp.*, 216 So.3d 346, 361 (La. Ct. App. 2017) (a buyer must allege that a product "is either absolutely useless . . . or so inconvenient or imperfect that, judged by the reasonable person standard . . . had he known of the defect, he never would have purchased it") (internal quotation marks and citation omitted). Hauck also does not allege that any security vulnerability rendered her processor "useless," only that the processor ran more slowly after she installed Spectre patches that third parties—not AMD—released. La. Civ. Code art. § 2520. As the Court has explained in its prior order, "[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Iqbal*, 556 U.S. at 678. Because Hauck's allegations remain entirely conclusory, the Court grants AMD's motion to dismiss the redhibition claim.

The Court finds that granting Plaintiffs leave to amend the redhibition claim would be futile and unduly prejudicial to AMD. *Leadsinger, Inc.*, 512 F.3d at 532. In its prior Order dismissing Plaintiffs' CAC, the Court dismissed Plaintiffs' redhibition claim because Hauck's

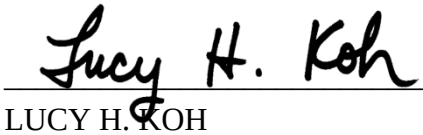
allegations parroted the elements of a redhibition claim. MTD Order at 17–18. The Court warned that "failure to cure the deficiencies identified in this Order will result in dismissal with prejudice." *Id.* at 20. Plaintiffs' SCAC suffers from the same deficiencies as the CAC. Because any further amendment would be futile, and it would be unduly prejudicial to AMD to litigate a third motion to dismiss regarding the same deficiencies—especially given the voluminous claims in this case—the Court DENIES Plaintiffs leave to amend their redhibition claim.

IV. CONCLUSION

For the foregoing reasons, the Court GRANTS AMD's motion to dismiss with prejudice all seven causes of action the parties have elected to litigate through summary judgment: (1) Count III for unfair practices under California's UCL; (2) Count V for fraud by omission; (3) Count VII for breach of express warranty; (4) Count VIII for breach of the implied warranty of merchantability; (5) Count XI for violation of FDUTPA; (6) Count XVII for redhibition; and (7) Count XIX for violation of the MCPA.

IT IS SO ORDERED.

Dated: April 4, 2019



LUCY H. KOH
United States District Judge