

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

DARQUES SMITH, et al.,
Plaintiffs,
v.
INTEL CORPORATION,
Defendant.

Case No. [23-cv-05761-HSG](#)

**ORDER GRANTING DEFENDANT’S
MOTION TO DISMISS,
TERMINATING AS MOOT
DEFENDANT’S MOTION TO STAY
DISCOVERY, AND IMPOSING
TEMPORARY DISCOVERY STAY**

Re: Dkt. Nos. 30, 33

Pending before the Court are Defendant’s motions to dismiss and to stay discovery pending resolution of the motion to dismiss. Dkt. Nos. 30, 33. The Court finds these matters appropriate for disposition without oral argument and the deems them submitted. *See* Civil L.R. 7-1(b). For the reasons discussed below, the Court **GRANTS** Defendant’s motion to dismiss, **TERMINATES AS MOOT** Defendant’s motion to stay discovery, and temporarily **STAYS DISCOVERY** until Plaintiffs allege an actionable claim.

I. BACKGROUND

On November 11, 2023, Darques Smith, Renee Waltrip, Brian Cameron, Elizabeth Cordova and Michael Worley, on behalf of themselves and all others similarly situated nationwide (“Plaintiffs”), filed a class action complaint against Intel Corporation (“Defendant”). *See* Dkt. No. 1 (“Compl.”). Plaintiffs – who purchased central processing units (“CPUs”) and computers incorporating CPUs made by Defendant – allege that Defendant knowingly sold CPUs with a security vulnerability. *Id.* ¶ 1, 5. According to Plaintiffs, Defendant was on notice of a hardware defect that created this security threat, but nevertheless continued to sell CPUs without fixing the root cause or disclosing the alleged defect. Moreover, Plaintiffs allege that Defendant knew that

United States District Court
Northern District of California

1 the only way to fix a hardware issue of the sort alleged would be to deploy software “patches” that
2 throttled the processing power of the CPUs.

3 At a high level, the security vulnerability that Plaintiffs allege relates to a computer
4 processing technique called “branch prediction.” According to Plaintiffs, branch prediction is a
5 “speculative procedure” developed in the 1990s designed to overcome barriers to speedy
6 computing caused by slow memory retrieval. *Id.* ¶ 75. Without branch prediction, “a CPU that
7 sequentially executes instructions will encounter a conditional instruction – one dependent on a
8 value stored in memory,” and “must wait until that value is fetched from memory (which is
9 relatively slow to access) to continue execution.” *Id.* ¶ 76. Branch prediction gets around this
10 time lag by “predict[ing] what a program will likely do when the processor encounters a
11 conditional instruction (i.e., an instruction dependent on some in-memory value).” *Id.* ¶ 77. A
12 specific technique for implementing branch prediction is called “speculative execution,” which
13 Plaintiffs allege is “an inherent part of a modern CPU’s computation process” on which modern
14 CPU performance depends. *Id.* ¶ 82. Plaintiffs allege that speculative execution works as follows:

15 [F]aced with a conditional instruction – i.e., an instruction based on a
16 value that must be retrieved – a CPU guesses what the value will be
17 instead of waiting for its retrieval from memory, and executes code
18 based on that guess. If, when the memory contents are fetched, the
19 guess is incorrect, the CPU discards the “speculative” code. If the
20 guess was right, the CPU has already executed past the conditional
instruction (e.g., conditional branch) without waiting, obviating the
need to wait for memory or system input/output to continue executing.

21 *Id.* ¶ 80. In short, speculative execution allows processors to “speculate on future instruction
22 directions and proactively execute instructions along these paths before knowing if the instructions
23 are correct,” and to deliver performance gains when the speculative instruction correctly matches
24 the value ultimately retrieved from the CPU memory. *Id.* ¶ 84.

25 But the guessed instructions – referred to as “transient instructions” – apparently must be
26 “completely cleared” from the CPU’s short-term memory after execution. *Id.* ¶ 83. A CPU’s
27 failure to flush transient instructions leaves “side effects” (i.e. lingering data) that can cause
28 “serious security problems,” according to Plaintiffs. *Id.* ¶ 84. The security problems arise from the

1 fact that the privileged data retrieved from the CPU’s memory to facilitate instruction execution
2 can become accessible to and exploitable by other parts of the computer which should not have
3 that access to that privileged data if retained by the CPU. *Id.* ¶¶ 90, 95.

4 Plaintiffs allege that Defendant’s hardware design is defective in that “it fails to ensure that
5 side effects of [transient] instructions do not linger in various parts of the CPU accessible to the
6 running program.” *Id.* ¶ 89. Instead of properly flushing these instructions, Defendant’s CPUs
7 allegedly “cause the CPU’s cache to store memory information previously required by
8 speculatively executed code, meaning that even if the transient code is discarded, some data
9 remains in the CPU’s cache.” *Id.* ¶ 90. Additionally, Defendant’s CPUs supposedly also use
10 “instruction buffers, where transient code may store information associated with particular
11 instructions. *Id.* ¶ 91. Plaintiffs allege that Intel’s failure to “ensure that transient code is
12 prevented from making lingering changes to shared CPU resources” makes its CPUs vulnerable to
13 a class of attacks called transient execution attacks. *Id.* ¶ 92.

14 According to Plaintiffs, the CPUs’ susceptibility to this novel class of attacks was publicly
15 revealed in 2018, after researchers at Google identified vulnerabilities they dubbed “Spectre” and
16 “Meltdown.” *Id.* ¶ 97. Spectre and Meltdown are “‘transient execution’ attacks, meaning that they
17 exploit the side effects of speculative code generated during speculative execution like branch
18 prediction.” *Id.* ¶ 101. Importantly, these vulnerabilities “can be exploited to steal sensitive data
19 present in a computer system’s memory.” *Id.* ¶ 98. And according to Plaintiffs, Spectre and
20 Meltdown were but two of a “larger class of vulnerabilities” arising from Defendant’s hardware
21 design of its branch prediction and segmentation systems. *Id.* ¶¶ 109, 115.

22 In response to the discovery of the Spectre and Meltdown attacks, Defendant deployed
23 software updates (or “patches”) to address the security vulnerability supposedly endemic to the
24 hardware. But according to Plaintiffs, Defendant’s mitigation “essentially handicapped the
25 functionality in Intel CPUs used to predict branches, to speculatively execute code, and to execute
26 code out of order.” *Id.* ¶ 120. Plaintiffs allege that *Wired* reported in March 2018 that “attempts to
27 disable [the vulnerability] at the software level can have a marked performance cost” – namely,
28 significantly reduced computing speeds. *Id.* ¶¶ 121, 126. The only solution to the transient

1 execution attacks, according to *Wired*, was to “physically replace all the chips, a change which will
2 take at least a full hardware generation to propagate.” *Id.* ¶ 119. Plaintiffs allege that Intel said it
3 would do just that: in a March 15, 2018 press release, Intel CEO Brian Krzanich allegedly
4 promised “a new hardware design in future chips to finally deal with the Spectre/Meltdown class
5 of vulnerability, including Spectre and Meltdown variants,” and indicated that design would be
6 incorporated into 8th generation chips by late 2018. *Id.* ¶ 126.¹

7 Plaintiffs allege that “Intel’s 2018 hardware redesign to overcome Spectre and Meltdown
8 vulnerabilities would need to secure its [Advanced Vector Extension] instructions, along with
9 other attack vectors,” and that Intel knew that. *Id.* ¶¶ 134. As Plaintiffs explain, “[a] vector
10 instruction is a CPU instruction that can perform the same type of operations on multiple data
11 samples in a particularly efficient manner,” and is “central to the performance and function of any
12 high-end CPU.” *Id.* ¶¶ 131, 132. Plaintiffs allege that in mid-2018, while Defendant was
13 undertaking its reengineering to address the Spectre and Meltdown class of attacks, Defendant
14 became aware of its CPUs’ Advanced Vector Extension (“AVX”) instructions being vulnerable to
15 side-channel attacks of the type exploited for Spectre/Meltdown. *Id.* ¶ 135. One “hardware
16 enthusiast” developed and reported to Defendant in June 2018 an exploit he called “AVX Clock
17 Spectre,” which, like the original Spectre attack, “exploited side effects left over from a predicted
18 branch of execution.” *Id.* ¶ 138. Around that time, “another AVX-based transient execution
19 exploit emerged, called NetSpectre.” *Id.* ¶ 145. Plaintiffs allege that “despite multiple (publicly
20 known) vulnerability disclosures made to Intel on the subject, Intel did not carefully analyz[e]
21 possible side-effects in the AVX [instructions] and engineering hardware solutions to fix them in
22 2018.” *Id.* ¶ 151. Instead, Plaintiffs allege that “Intel put profits first, selling defective CPUs for
23 years after it clearly knew them to be defective, and knew that the hardware implementation of
24 Intel’s branch prediction systems needed to be addressed to prevent leaking side effects from
25 speculative execution – specifically as to Intel’s AVX instructions.” *Id.*

26 _____
27 ¹ As the Court explains more fully below, the revelations about the Meltdown and Spectre
28 vulnerabilities (experienced not only by Intel but also Apple and Advanced Microdevices
 (“AMD”)) and the throttling mitigations they required spurred at least three lawsuits in district
 courts in the Ninth Circuit.

1 Plaintiffs allege that Defendant’s failure to address the root cause led to the “inevitable”: in
2 August 2023, Defendant publicly acknowledged a new vulnerability called “Downfall,” which
3 “allowed an attacker to launch a transient execution attack using Intel’s AVX instructions and side
4 effects left by Intel’s defective branch prediction system.” *Id.* ¶¶ 153–54. While Plaintiffs’
5 complaint alleges many additional technical facts about the nature of this attack, the bottom line is
6 their allegation that the attack emerged because Intel “had done nothing to safeguard against the
7 CPUs’ cache retaining what should have been discarded data resulting from speculative
8 execution,” even though it allegedly knew that the Spectre and Meltdown attacks exploited similar
9 vulnerabilities and had allegedly received direct warnings in Summer 2018 regarding the AVX
10 instruction set. *Id.* ¶ 167. The lack of root-cause hardware solutions is reflected, Plaintiffs allege,
11 by the fact that Intel’s 9th through 11th generation chips were vulnerable to Downfall even though
12 they “were supposed to have received hardware redesigns that would fix the class of vulnerabilities
13 associated with Spectre, Meltdown, and other transient execution attacks.” *Id.* ¶ 176.

14 Plaintiffs allege that the mitigations Intel released to address the “incurable vulnerability”
15 of Downfall was a “medicine . . . on par with the disease.” *Id.* ¶¶ 182, 184. These mitigations
16 purportedly “destroyed CPU performance for certain, critical processing tasks,” causing
17 “performance degradation” of up to 50% that users could not easily avoid. *Id.* ¶ 184. Plaintiffs
18 allege that this degree of CPU impairment makes Defendant’s products “unmarketable” because
19 “[a]ll modern CPUs rely on sophisticated branch prediction, speculative execution, and out-of-
20 order execution to achieve expected performance characteristics.” *Id.* ¶ 196.

21 Based on Defendant’s conduct, Plaintiffs allege violations of the Unfair Competition Law
22 (“UCL”) (Cal. Bus. & Prof. Code § 17200, et seq.), Consumer Legal Remedies Act (“CLRA”)
23 (Cal. Civ. Code § 1750, et seq.), and False Advertising Law (“FAL”) (Cal. Bus. & Prof. Code §
24 17500, et seq.), and assert claims for fraud by omission, quasi-contract/restoration, negligence, and
25 breach of implied warranty under Cal. Comm. Code § 2314 and the Song-Beverly Consumer
26 Warranty Act (Cal. Civ. Code § 1790, et seq.). In the event a nationwide class is not certified,
27 Plaintiffs also bring in the alternative a variety of claims under Oregon, Kansas, Illinois, and
28 Minnesota law that more or less correspond with the California law violations alleged on behalf of

1 the entire class.²

2 On January 25, 2024, Defendant filed a motion to dismiss Plaintiffs’ entire complaint and
3 shortly thereafter, a motion to stay discovery. *See* Dkt. Nos. 30 (“MTD”), 33 (“Stay Mot.”). The
4 motions are fully briefed. *See* Dkt. No. 42 (“MTD Opp”), 43 (“MTD Reply”), 40 (“Opp. Stay
5 Mot.”), 41 (“Reply Stay Mot.”).

6 **II. LEGAL STANDARD**

7 Federal Rule of Civil Procedure 8(a) requires that a complaint contain “a short and plain
8 statement of the claim showing that the pleader is entitled to relief.” Fed. R. Civ. P. 8(a)(2). A
9 defendant may move to dismiss a complaint for failing to state a claim upon which relief can be
10 granted under Rule 12(b)(6). “Dismissal under Rule 12(b)(6) is appropriate only where the
11 complaint lacks a cognizable legal theory or sufficient facts to support a cognizable legal theory.”
12 *Mendondo v. Centinela Hosp. Med. Ctr.*, 521 F.3d 1097, 1104 (9th Cir. 2008). To survive a Rule
13 12(b)(6) motion, a plaintiff need only plead “enough facts to state a claim to relief that is plausible
14 on its face.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). A claim is facially plausible
15 when a plaintiff pleads “factual content that allows the court to draw the reasonable inference that
16 the defendant is liable for the misconduct alleged.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009).

17 Rule 9(b) imposes a heightened pleading standard where fraud is an essential element of a
18 claim. *See* Fed. R. Civ. P. 9(b) (“In alleging fraud or mistake, a party must state with particularity
19 the circumstances constituting fraud or mistake.”); *see also Vess v. Ciba–Geigy Corp. USA*, 317
20 F.3d 1097, 1107 (9th Cir. 2003). A plaintiff must identify “the who, what, when, where, and how”
21 of the alleged conduct, so as to provide defendants with sufficient information to defend against
22 the charge. *Cooper v. Pickett*, 137 F.3d 616, 627 (9th Cir. 1997). However, “[m]alice, intent,
23 knowledge, and other conditions of a person’s mind may be alleged generally.” Fed. R. Civ. P.
24 Rule 9(b).

25 In reviewing the plausibility of a complaint, courts “accept factual allegations in the

26 _____
27 ² Because the Oregon, Kansas, Illinois, and Minnesota state law claims were pled in the alternative
28 (in the event that the Court does not certify a nationwide class and instead permits state-based subclasses), and given that Defendant’s motion only cursorily addresses any of these non-California claims, the Court declines to address them at this time.

1 complaint as true and construe the pleadings in the light most favorable to the nonmoving party.”
2 *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008). Nevertheless,
3 courts do not “accept as true allegations that are merely conclusory, unwarranted deductions of
4 fact, or unreasonable inferences.” *In re Gilead Scis. Secs. Litig.*, 536 F.3d 1049, 1055 (9th Cir.
5 2008) (quoting *Sprewell v. Golden State Warriors*, 266 F.3d 979, 988 (9th Cir. 2001)).

6 Even if the court concludes that a 12(b)(6) motion should be granted, the “court should
7 grant leave to amend even if no request to amend the pleading was made, unless it determines that
8 the pleading could not possibly be cured by the allegation of other facts.” *Lopez v. Smith*, 203
9 F.3d 1122, 1127 (9th Cir. 2000) (en banc) (quotation omitted).

10 **III. DISCUSSION**

11 **A. Request for Judicial Notice**

12 Along with its motion to dismiss, Defendant filed a request for judicial notice. *See* Dkt.
13 No. 31. The Court will **GRANT** the request.

14 **i. Standard**

15 In *Khoja v. Orexigen Therapeutics*, the Ninth Circuit clarified the judicial notice rule and
16 incorporation by reference doctrine. *See* 899 F.3d 988 (9th Cir. 2018). Under Federal Rule of
17 Evidence 201, a court may take judicial notice of a fact “not subject to reasonable dispute because
18 it . . . can be accurately and readily determined from sources whose accuracy cannot reasonably be
19 questioned.” Fed. R. Evid. 201(b)(2). Accordingly, a court may take “judicial notice of matters of
20 public record,” but “cannot take judicial notice of disputed facts contained in such public records.”
21 *Khoja*, 899 F.3d at 999 (citation and quotations omitted). The Ninth Circuit has clarified that if a
22 court takes judicial notice of a document, it must specify what facts it judicially noticed from the
23 document. *Id.* at 999. Further, “[j]ust because the document itself is susceptible to judicial notice
24 does not mean that every assertion of fact within that document is judicially noticeable for its
25 truth.” *Id.* As an example, the Ninth Circuit held that for a transcript of a conference call, the
26 court may take judicial notice of the fact that there was a conference call on the specified date, but
27 may not take judicial notice of a fact mentioned in the transcript, because the substance “is subject
28 to varying interpretations, and there is a reasonable dispute as to what the [document] establishes.”

1 *Id.* at 999–1000.

2 **ii. Analysis**

3 Defendant moves the Court to take judicial notice of seven exhibits referenced in its
4 motion to dismiss. Exhibits 1, 2, and 7 contain publicly available government or government-
5 affiliated webpages, and Exhibit 3 contains a document (“NCCIC Services for Federal Agencies”)
6 downloaded from a government-maintained website (www.CISA.gov). Exhibits 4, 5, and 6 reflect
7 excerpts from complaints filed in *In re Intel Corp. CPU Marketing, Sales Practices & Products*
8 *Liability Litigation*, No. 18-md-2828 (D. Or.), ECF No. 209 and *Hauck v. Advanced Micro*
9 *Devices, Inc.*, No. 18-cv-00447 (N.D. Cal.), ECF Nos. 53, 95 – prior cases against Intel and its
10 competitor AMD relating to the Spectre and Meltdown attacks. All of these materials are
11 judicially noticeable, as the accuracy of their contents is not subject to reasonable dispute. *See,*
12 *e.g., Threshold Enters. Ltd. v. Pressed Juicery, Inc.*, 445 F. Supp. 3d 139, 146 (N.D. Cal. 2020)
13 (taking judicial notice of websites and their contents), *Est. of Blue v. Cnty. of L.A.*, 120 F.3d 982,
14 984 (9th Cir. 1997) (affirming that court may take judicial notice of filings in other cases).
15 Accordingly, the Court will **GRANT** Defendant’s request. However, in keeping with *Khoja*, the
16 Court will consider the materials’ contents but will not assume their truth.

17 **B. Motion to Dismiss**

18 **i. Prior Litigation**

19 Before turning to the merits of the motion before it, the Court acknowledges that this is not
20 the first challenge relating to side-channel attacks on CPUs. Following the revelations about the
21 Spectre and Meltdown vulnerabilities in 2018, various plaintiffs filed suit against Intel and other
22 chip manufacturers such as Apple and AMD alleging claims similar to those pressed here. All of
23 these cases were eventually dismissed with prejudice after numerous opportunities for leave, and
24 those dismissals were ultimately affirmed by the Ninth Circuit in unpublished decisions. *See*
25 *Hauck v. Advanced Micro Devices, Inc.*, No. 18-CV-00447-LHK, 2019 WL 1493356 (N.D. Cal.
26 Apr. 4, 2019), *aff’d*, 816 F. App’x 39 (9th Cir. 2020); *In re Apple Processor Litig.*, No. 18-CV-
27 00147-EJD, 2022 WL 2064975 (N.D. Cal. June 8, 2022), *aff’d*, No. 22-16164, 2023 WL 5950622
28 (9th Cir. Sept. 13, 2023); *In re Intel Corp. CPU Mktg., Sales Pracs. & Prod. Liab. Litig.*, 614 F.

1 Supp. 3d 783 (D. Or. 2022), *aff'd*, No. 22-35652, 2023 WL 7211394 (9th Cir. Nov. 2, 2023).

2 Defendant makes much of this litigation history, arguing that the failure of prior claims
3 foretells the failure of these claims. Because this framing device is so pervasive in Defendant’s
4 briefing, the Court clarifies at the outset that the allegations in this case are not identical to those at
5 issue in the prior cases. Whereas plaintiffs in the first wave of litigation bought their CPUs before
6 the vulnerability at issue publicly came to light in 2018, Plaintiffs here bought their devices after
7 that juncture. In other words, their claims are not rooted in the post-sale emergence of a novel
8 CPU vulnerability, but rather in Defendant’s alleged pre-sale maintenance of that then-known
9 vulnerability. While that factual distinction certainly does not guarantee that any of Plaintiffs’
10 claims survive, it makes the outcomes of the prior cases informative rather than strictly inevitable.

11 **ii. Fraud Claims**

12 Plaintiffs plead claims for fraud-based violations of the FAL, CLRA, and UCL, as well as
13 common law fraud by omission. Defendant moves to dismiss, arguing that Plaintiffs’ claims
14 sounding in fraud have not been pled with particularity, as required by Rule 9(b).³ *See Kearns v.*
15 *Ford Motor Co.*, 567 F.3d 1120, 1125 (9th Cir. 2009). Considering the arguments presented and
16 construing the pleadings in the light most favorable to Plaintiffs, as it must, the Court is persuaded
17 that dismissal of these omission-based claims is appropriate. Though a close call, the Court finds
18 that Plaintiffs have not done enough to allege an actionable omission under the heightened
19 pleading standard imposed by Rule 9(b).⁴

20 Under California law, omissions that form the basis of claims brought under state
21 consumer protection laws “‘must be contrary to a representation actually made by the defendant,
22 or an omission of a fact the defendant was obliged to disclose.’” *Hodsdon v. Mars*, 891 F.3d 857,
23 861 (9th Cir. 2018) (quoting *Daugherty v. Am. Honda Motor Co.*, 144 Cal. App. 4th 824, 835

24 _____
25 ³ Defendant also moves to dismiss the claims brought in the alternative under Oregon, Kansas,
26 Illinois, and Minnesota consumer protection laws. At this juncture, the Court declines to evaluate
27 the viability of these or any alternative claims Defendant moves to dismiss.

28 ⁴ For reasons that are not clear to the Court, Plaintiffs do not allege any affirmative
misrepresentation theory, even as they imply that Intel did not do what it purportedly publicly
promised to do. *See* Compl. ¶¶ 126, 129–30. And even as to the omission theory, Plaintiffs do not
specify what marketing material or other communications by Defendant and relied upon by
Plaintiffs failed to disclose the alleged defect.

1 (2006) (emphasis omitted)). “In *Hodsdon*, the Ninth Circuit – synthesizing recent decisions of the
2 California Courts of Appeal – explained that a plaintiff sufficiently pleads a duty to disclose
3 where: (1) the plaintiff alleges the omission was material; (2) the alleged defect was central to the
4 product’s function; and (3) the defendant (a) is plaintiff’s fiduciary, (b) has ‘exclusive knowledge’
5 of material facts, (c) ‘actively conceals’ a material fact, or (d) makes misleading partial
6 representations.” *In re Natera Prenatal Testing Litig.*, 664 F. Supp. 3d 995, 1008 (N.D. Cal.
7 2023) (quoting *id.* at 863); *see also LiMandri v. Judkins*, 52 Cal. App. 4th 326, 337 (1997) (laying
8 out factors listed in (3), referred to as “*LiMandri* factors”).

9 Defendant argues that Plaintiffs do not adequately plead that the omission at issue is
10 material. Specifically, Intel contends that the defect could not have had any bearing on Plaintiffs’
11 purchase decisions since they bought their CPUs (or computers containing CPUs) after the Spectre
12 and Meltdown news became public in 2018. MTD at 22. But this argument reveals that
13 Defendant either misapprehends or misconstrues the omission about which Plaintiffs complain.
14 *See* MTD at 22–23. Unlike the parties in prior litigation, Plaintiffs’ complaint is focused not on
15 the emergence of the Spectre and Meltdown attacks in 2017 (which was publicly revealed in
16 2018), but on Defendant’s supposed failure from 2018 onward to address and disclose allegedly
17 known hardware defects – including those affecting the AVX instructions – that allegedly allowed
18 this class of vulnerabilities to persist and ultimately culminate in Downfall. This focus is reflected
19 in Plaintiffs’ allegations: Plaintiffs plead that if Intel had disclosed that the speculative execution
20 vulnerabilities revealed in 2018 had not been remediated in the CPU models they purchased,
21 Plaintiffs would not have paid what they did for the products. *See* Compl. ¶¶ 24, 28, 32, 36. To
22 underscore this point, Plaintiffs allege that they conducted conjoint studies tending to show that
23 “consumers are willing to pay significantly less for a computer with an affected Intel CPU”
24 because an affected Intel CPU “loses 85% of its value because of the security vulnerability.” *Id.* ¶
25 228, 229. At this early stage, these allegations sufficiently allege materiality.

26 As for centrality of the defect, Plaintiffs are required to plead that “the allegedly concealed
27 *physical* defect was *central* to the product’s function.” *Hodsdon*, 891 F.3d at 864 (emphasis in
28 original). The alleged central functionality of a defect cannot be based on “subjective

1 preferences” about a product, but rather must render those products “incapable of use by any
 2 consumer.” *Id.* For instance, while one person may have “no practical use” for a chocolate bar
 3 tainted by slave or child labor, “some consumers of chocolate are not concerned about the labor
 4 practices used to manufacture the product.” *Id.* Because a supply chain tarnished by labor
 5 violations did not therefore render the chocolate at issue “incapable of use by any consumer,”
 6 *Hodsdon* did not find for the plaintiff. *Id.* Following *Hodsdon*, district courts have implemented
 7 the central functionality test with some variation: some focus more on whether the alleged defect
 8 affects the product’s central function “even if the product still retains overall functionality and
 9 use,” and others apply the “incapable of use by any consumer” test, based on the phrasing used in
 10 *Hodsdon*. See *In re Intel Corp. CPU Mktg., Sales Pracs. & Prod. Liab. Litig.*, No. 3:18-MD-
 11 2828-SI, 2021 WL 1198299, at *8 (D. Or. Mar. 29, 2021) (“*Intel II*”) (summarizing different
 12 approaches).

13 Defendant argues that while the “incapable of use” standard is correct, Plaintiffs’
 14 allegations fail to satisfy either test. MTD at 19. It contends that “Plaintiffs do not, and cannot,
 15 allege that the ‘defect’ renders Intel CPUs incapable of performing their central function, which is
 16 to process instructions.” MTD at 20. The Court ultimately agrees, and finds the rulings in *Intel II*
 17 instructive. In reviewing Intel’s second motion to dismiss, the district court presiding over that
 18 action observed that “[e]ven if the [central functionality] test does not require that the defect
 19 render the product incapable of use by any consumer, the Ninth Circuit was clear in *Hodsdon* that
 20 the defect must be central and important to the product’s function.” *Intel II*, 2021 WL 1198299 at
 21 8. While plaintiffs in that case described the CPU’s central function as “processing securely,” the
 22 *Intel* court was not satisfied that plaintiffs’ allegations demonstrated that the defect – which was,
 23 as it is here, “increased vulnerability to potential cache side-channel attacks” – actually affected
 24 the CPUs’ *processing* capabilities. *Id.* As a result, the *Intel* court found that the alleged defect did
 25 not “go to the *central function* of the microprocessors” because even with the latent security
 26 vulnerability, Intel’s chips were able to “perform[] as the ‘brains’ of the devices in which they are
 27 placed.” *Id.* (emphasis in original). This ruling was ultimately affirmed in a Ninth Circuit
 28 memorandum disposition, which held that the district court’s finding was appropriate given that

1 plaintiffs did not allege that their processors ever “stopped operating as ‘the brains of the
2 computing device[s].” *In re Intel Corp. CPU Mktg., Sales Pracs. & Prod. Liab. Litig.*, No. 22-
3 35652, 2023 WL 7211394, at *1 (9th Cir. Nov. 2, 2023).⁵ The Ninth Circuit also observed that
4 while security vulnerabilities “may well be material to consumers, the security risk presented by
5 the defects alleged . . . does not make those defects central to the processors’ function.” *Id.*

6 Plaintiffs in this case argue that they have met the standard suggested by the Ninth Circuit
7 in *In re Intel* because they have pled that “the CPUs Intel sold Plaintiffs are defective because they
8 do not operate as ‘the brains’ of the computing device and do not perform ‘all necessary
9 computations for each application’ and for ‘each peripheral.’” MTD Opp. at 17. The rub, as
10 Defendant points out, is that Plaintiffs have not actually made those allegations. While they have
11 certainly alleged that the defect impairs AVX vector instructions and a CPU’s segmentation
12 functionality, Plaintiffs’ allegations do not plausibly suggest that impairment of these features
13 causes a CPU to cease operating as the “brains” of a computer. Based on the reasoning adopted in
14 *Intel II*, which this Court finds persuasive, the lack of allegations connecting the latent security
15 defect to core *processing* capabilities sinks Plaintiffs’ claim.⁶ Since Plaintiffs have not adequately
16 pled that the alleged defect was central to the functionality of Intel’s microprocessors, the Court
17 can conclude that Plaintiffs have not properly alleged an actionable omission claim, and need not
18 assess whether any *LaMandri* factors are adequately pled.

19 Accordingly, the Court **GRANTS** Defendant’s motion to dismiss Plaintiffs’ fraud-based
20 FAL, UCL, CLRA, and common law claims.

21 **iii. Quasi-Contract/Unjust Enrichment**

22 Defendant moves to dismiss Plaintiffs’ claims for quasi-contract and unjust enrichment.

24 ⁵ As an unpublished Ninth Circuit decision, *In re Intel* is not precedent, but may be considered for
25 its persuasive value. See Fed. R. App. P. 32.1; CTA9 Rule 36-3.
26 ⁶ As should be clear from this conclusion, the Court does not view the software mitigation patch as
27 an additional or related defect. The patch was not a part of the product at the time of sale, and
28 while Plaintiffs allege that Defendant knew that a patch would be required to address hardware
defects, the Court does not find it plausibly alleged that deploying a performance-reducing patch
in the future was assured or inevitable at the time of sale. Instead, from that vantage point in time,
the only defect was the alleged security vulnerability to side-channel attacks that Plaintiffs allege
was endemic to Defendant’s CPU hardware design.

1 Although there is no standalone cause of action in California for “unjust enrichment,” courts may
2 “construe [a claim for unjust enrichment] as a quasi-contract claim seeking restitution.” *Astiana v.*
3 *Hain Celestial Grp., Inc.*, 783 F.3d 753, 762 (9th Cir. 2015).

4 Plaintiffs contend that restitution is due to them because Intel knew “that the Affected Intel
5 CPUs, and computers built around them, were actually worth substantially less than the price they
6 were sold for” as a result of their unreasonable insecurity, but nevertheless failed to provide any
7 “discount or disclosure to account for their actual, degraded” condition. MTD Opp. at 29. With
8 this claim, Plaintiffs seek disgorgement of that allegedly wrongfully retained premium. Defendant
9 argues that because Plaintiffs failed to plead an actionable omission, their efforts to recover
10 restitution under a quasi-contract theory must also fail, since Defendant’s retention of benefits is
11 not “unjust or inequitable.” MTD at 29. The Court agrees. “[A] restitution claim based on fraud
12 or consumer protection claims must nonetheless be dismissed if the plaintiff fails to sufficiently
13 plead an actionable misrepresentation or omission.” *In re Apple Processor Litig.*, No. 18-CV-
14 00147-EJD, 2022 WL 2064975, at *12 (N.D. Cal. June 8, 2022), *aff’d*, No. 22-16164, 2023 WL
15 5950622 (9th Cir. Sept. 13, 2023). Here, as in *In re Apple*, Plaintiffs’ “unjust enrichment claim
16 relies on the same set of allegations as Plaintiffs’ [f]raud [c]laims addressed above, namely that
17 [Intel] fraudulently omitted information regarding the [security defect],” such that “their unjust
18 enrichment claim relying on the same alleged fraudulent conduct must also be dismissed.” *Id.*
19 Defendant’s motion is **GRANTED** on this theory.

20 **iv. Negligence**

21 Defendant moves to dismiss Plaintiffs’ claim for negligence. The Court will **GRANT** the
22 motion on this theory.

23 To state a claim for negligence under California law, a plaintiff must establish (1) duty, (2)
24 breach of duty, (3) causation, and (4) damages. *See Merrill v. Navegar, Inc.*, 26 Cal. 4th 465, 500
25 (Cal. 2001). However, “plaintiffs asserting negligence claims ordinarily may not recover purely
26 economic damages unconnected to physical injury or property damage Economic losses
27 include damages for inadequate value, costs of repair, loss of expected proceeds, loss of use, loss
28 of goodwill, and damages paid to third parties.” *Castillo v. Seagate Tech., LLC*, 2016 WL

1 9280242, at *5 (N.D. Cal. Sept. 14, 2016). This is the economic loss doctrine. “But ‘California
 2 decisional law has long recognized that the economic loss rule does not necessarily bar recovery in
 3 tort for damage that a defective product . . . causes to other portions of a larger product . . . into
 4 which the former has been incorporated.’” *Hauck v. Advanced Micro Devices, Inc.*, No. 18-CV-
 5 00447-LHK, 2018 WL 5729234, at *10 (N.D. Cal. Oct. 29, 2018) (“AMD I”) (quoting *Jimenez v.*
 6 *Superior Ct.*, 29 Cal. 4th 473, 483 (2002)). Nonetheless, if the damage to the larger product was
 7 “closely related” to the nature of the defect, then the economic loss doctrine may still prevent
 8 recovery. *See In re Sony Vaio Computer Notebook Trackpad Litig.*, No. 09CV2109 BEN RBB,
 9 2010 WL 4262191, at *7 (S.D. Cal. Oct. 28, 2010) (finding economic loss doctrine applicable in
 10 case where “trackpad was integral to the function of the notebook,” “any damage to the notebook,
 11 i.e. erratic tracking and freezing, was closely related to the nature of the defect in the trackpad,”
 12 and allegations lacked any suggestion that “a trackpad would have any use to Plaintiffs outside of
 13 the notebooks.”). In other words, “[w]hen the defect and the damage are one and the same, the
 14 defect may not be considered to have caused physical injury.” *KB Home v. Superior Ct.*, 112 Cal.
 15 App. 4th 1076, 1085 (2003) (internal quotations omitted) (citing *Sacramental Regional Transit*
 16 *Dist. v. Grumman Flxible*, 158 Cal. App. 3d 289, 294 (1984)).

17 Defendant argues that the economic loss doctrine bars Plaintiffs’ claims, and that Plaintiffs
 18 have not adequately pled that Defendant breached the standard of care. MTD at 28–29. Plaintiffs
 19 respond that their allegations not only detail breach, but also describe how the affected CPUs
 20 caused property damage to the computers that incorporated them, thereby circumventing the
 21 economic loss doctrine. MTD Opp. at 30–32. Because Defendant has the better of the arguments
 22 as to the applicability of the economic loss doctrine, the Court does not reach the standard of care
 23 question. As to physical injury allegedly caused by the CPUs, Plaintiffs plead that Defendant’s
 24 negligently designed CPUs led to “diminished battery life (for laptops) and (for all computers) a
 25 diminished expected life for the CPU and nearby components due to the CPU running for longer
 26 and at hotter temperatures.” Compl. ¶ 408. But based on the nature of the relationship between
 27 the CPU and the computer – with the latter physically incorporating the former and deriving its
 28 core functionality from it – the Court agrees with Defendant that the CPUs are not “analytically

1 separate” from the computers they are in. *AMD I*, 2018 WL 5729234, at *11. Whether pre-
2 installed in Plaintiffs’ laptops or integrated by Plaintiffs into their computers, the affected CPUs
3 are “integrally tied” to other components and the computer overall such that they cannot
4 realistically be viewed as a standalone defective product harming another discrete piece of
5 property. *See id.* Because “Plaintiffs’ allegations indicate that the [computer], rather than the
6 [CPU] is the product at issue,” *In re Sony*, 2010 WL 4262191, at *7, Plaintiffs’ negligence claim
7 seeks to recover damages that are barred by the economic loss doctrine, and the Court will
8 accordingly **GRANT** Defendant’s motion to dismiss it.

9 **v. Breach of Implied Warranty**

10 Defendant moves to dismiss Plaintiffs’ nationwide breach of implied warranty of
11 merchantability claims, brought under California Commercial Code section 2314 and Civil Code
12 section 1790 (the Song-Beverly Consumer Warranty Act). The Court will **GRANT** the motion.

13 California law provides that “a warranty that the goods shall be merchantable is implied in
14 a contract for their sale if the seller is a merchant with respect to goods of that kind.” Cal. Com.
15 Code § 2314(1); *see also* Cal. Civ. Code § 1792 (establishing that “every sale of consumer goods
16 that are sold at retail in this state shall be accompanied by the manufacturer’s and the retail seller’s
17 implied warranty that the goods are merchantable”). The implied warranty of merchantability
18 “does not impose a general requirement that goods precisely fulfill the expectation of the buyer.
19 Instead, it provides for a minimum level of quality.” *Am. Suzuki Motor Corp. v. Superior Court*,
20 37 Cal. App. 4th 1291, 1296 (Cal. App. 1995) (internal quotation omitted). Rather, for an implied
21 warranty claim to survive a motion to dismiss, the plaintiff must plausibly allege that the product
22 at issue has manifested a problem so serious that it lacks “even the most basic degree of fitness
23 for ordinary use.” *Birdsong v. Apple, Inc.*, 590 F.3d 955, 958 (9th Cir. 2009) (quoting *Mocek v.*
24 *Alfa Leisure, Inc.*, 114 Cal. App. 4th 402, 406 (Cal. App. 2003)).

25 Defendant argues that Plaintiffs’ implied warranty claim fails for two reasons: first,
26 because Plaintiffs have not plausibly alleged that the affected CPUs lacked “even the most basic
27 degree of fitness for ordinary use,” and second, because of the nature of the third-party transaction.
28 MTD at 26–28, 30–31. While the Court is skeptical, based on Plaintiffs’ allegations, that the

1 CPUs at issue lack even a “basic degree of fitness,” it need not reach that question, as Defendant’s
 2 other arguments concerning the structure of the transaction convince the Court that the claim
 3 cannot proceed as pled. For one, it appears that Plaintiffs and Defendant are not in vertical privity,
 4 which is a strict requirement for breach of implied warranty claims under California law. *See*
 5 *Clemens v. DaimlerChrysler Corp.*, 534 F.3d 1017, 1024 (9th Cir. 2008). As explained in
 6 *Mandani v. Volkswagen Group of America, Inc.*, this Court, after carefully considering the circuit
 7 split on this issue, has not found a third-party beneficiary exception to these privity requirements.
 8 No. 17-CV-07287-HSG, 2019 WL 652867, at *5–6 (N.D. Cal. Feb. 15, 2019). As a result, since
 9 Plaintiffs Cameron and Waltrip – the only named Plaintiffs asserting this claim – allege that they
 10 purchased the products at issue from third-party retailers rather than from Defendant directly, the
 11 Court is of the view that Plaintiffs and Defendant are not “adjoining links in the distribution
 12 chain,” as required for this claim as a matter of California law. *Id.* at *5 (quoting *Clemens*, 534
 13 F.3d at 1023). Accordingly, the Court finds that their allegations do not state a claim.

14 Further, Plaintiffs do not plausibly plead that for purposes of California Civil Code section
 15 1792, the transactions at issue occurred in California. *See* Civ. Code § 1792 (“[E]very sale of
 16 consumer goods that are sold at retail *in this state*”) (emphasis added). Plaintiffs plead only
 17 that Cameron and Waltrip purchased their products from third party retailers named Microcenter
 18 and Newegg.com. Compl. ¶ 438. While Plaintiffs allege that Intel “is headquartered in California
 19 and directs its United States sales and shipping operations from California,” *id.* ¶ 430, there is no
 20 allegation that “Intel shipped anything to Cameron or Waltrip, or that Microcenter or NewEgg is
 21 affiliated with Intel in any way.” MTD Reply at 19. Without an allegation that makes plausible
 22 that Plaintiffs’ transactions with Microcenter or NewEgg occurred in California (with Intel or
 23 otherwise), the Court cannot conclude that the products at issue were “sold at retail *in this state*” as
 24 opposed to any other, as section 1792 requires.

25 Accordingly, the Court **GRANTS** Defendant’s motion to dismiss Plaintiffs’ implied
 26 warranty of merchantability claims.

27 **vi. UCL – Unfair and Unlawful Prongs**

28 Defendant moves to dismiss Plaintiffs’ claims under the unlawful and unfair prongs of the

1 UCL. The Court first considers Defendant’s arguments against Plaintiffs’ unfair prong claim.
 2 While the standard for unfair UCL claims is unsettled, *see Price v. Apple, Inc.*, No. 21-CV-02846-
 3 HSG, 2022 WL 1032472, at *4 (N.D. Cal. Apr. 6, 2022) (explaining competing standards),
 4 Plaintiffs allege that under one of the accepted balancing tests, Defendant’s practice is unfair
 5 because its “impact on [victim Plaintiffs] outweigh the reasons, justifications, and motives of
 6 [Intel,] the alleged wrongdoer.” *Doe v. CVS Pharmacy, Inc.*, 982 F.3d 1204 (9th Cir. 2020)
 7 (internal quotation omitted). Plaintiffs argue that their unfair claim does not rely on the viability
 8 of their fraud theory, asserting that “Intel’s decision to sell CPUs without the necessary
 9 mitigations to make them safe against a known vulnerability was an unfair practice – a practice
 10 distinct from Intel’s fraudulent omission.” MTD Opp. at 20. But the Court is not persuaded that
 11 the complaint reflects this distinction. In pleading their unfair UCL claim, Plaintiffs characterize
 12 as “unfair” Defendant’s failure to properly redesign its hardware after Spectre, Meltdown, and the
 13 warnings about the AVX instruction set, as well as its adoption of a mitigation patch that
 14 substantially impairs the operation of Defendant’s CPUs. It strikes the Court that there is little to
 15 no daylight between these allegations and the allegations supporting Plaintiffs’ fraud claims,
 16 which the Court found inactionable. Accordingly, since it does not adequately allege either a
 17 distinct, unfair practice or an actionable omission, the Court finds that Plaintiffs fail to allege
 18 conduct supporting a claim that Intel engaged in unfair conduct. *See Intel II*, 2021 WL 1198299 at
 19 *11. Accordingly, the Court **GRANTS** Defendant’s motion to dismiss this claim.

20 As for Defendant’s motion to dismiss Plaintiffs’ unlawful prong claim, the Court also
 21 **GRANTS** it. Plaintiffs can only survive a motion to dismiss claims brought under this prong if
 22 they plead sufficient facts to support another cause of action. *See Moran v. Prime Healthcare*
 23 *Mgmt., Inc.*, 3 Cal. App. 5th 1131, 1142 (2016). Since they have not, their UCL unlawful prong
 24 claim cannot survive Defendant’s motion to dismiss. *See Cullen v. Netflix, Inc.*, 880 F. Supp. 2d
 25 1017, 1028 (N.D. Cal. 2012) (Where “other claims fail, [the] UCL claims premised on ‘unlawful
 26 acts ha[ve] no basis and must also fail.”).

27 **A. Motion to Stay Discovery**

28 Defendant previously moved to stay discovery pending resolution of the motion to dismiss.


1 Dkt. No. 33. Seeing as the Court resolved the motion to dismiss before ruling on Defendant’s
2 motion for a temporary stay, the Court will **TERMINATE** Defendant’s motion as moot since the
3 relief it requests is no longer available. However, having found the underlying motion to dismiss
4 warrants dismissal of the complaint in its entirety, the Court finds that there is good cause to
5 temporarily stay discovery until it is clear if any claims will proceed based on Plaintiffs’
6 amendments. *See Rutman Wine Co. v. E. & J. Gallo Winery*, 829 F.2d 729, 738 (9th Cir. 1987)
7 (“It is sounder practice to determine whether there is any reasonable likelihood that plaintiffs can
8 construct a claim before forcing the parties to undergo the expense of discovery.”). Accordingly,
9 the Court will **STAY** discovery in this case until otherwise ordered.

10 **IV. CONCLUSION**

11 The Court **GRANTS** Defendant’s motions to dismiss, Dkt. No. 30 and **TERMINATES**
12 **AS MOOT** its motion to stay discovery pending resolution of that motion, Dkt. No. 33. Because
13 granting Plaintiffs an opportunity to amend their complaint would not be futile, cause undue delay,
14 or unduly prejudice Intel, and Plaintiffs have not acted in bad faith, the Court grants leave to
15 amend. Any amended complaint is due within 28 days of the date of this order. However, given
16 that Plaintiffs’ first consolidated class action complaint failed to state a viable claim, the Court
17 will **STAY DISCOVERY** until it is clear whether Plaintiffs can successfully cure the defects
18 identified in this order.

19 **IT IS SO ORDERED.**

20 Dated: 8/15/2024

21 
22 HAYWOOD S. GILLIAM, JR.
23 United States District Judge
24
25
26
27
28