

United States District Court  
Northern District of California

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  
SAN JOSE DIVISION

KEVIN RIORDAN, et al.,  
Plaintiffs,  
v.  
WESTERN DIGITAL CORPORATION,  
Defendant.

Case No. [5:21-cv-06074-EJD](#)

**ORDER GRANTING IN PART AND DENYING IN PART DEFENDANT’S MOTION TO DISMISS**

Re: ECF No. 40

Pending before this Court is Defendant Western Digital Corporation’s (“Western Digital”) motion to dismiss. ECF No. 40 (“Mot.”). The Court took the motion under submission for decision without oral argument pursuant to Civil Local Rule 7-1(b). For the reasons discussed herein, the Court GRANTS IN PART and DENIES IN PART Western Digital’s motion to dismiss with leave to amend.

**I. BACKGROUND**

Western Digital is a leading global and data storage brand incorporated in Delaware and headquartered in California. ECF No. 37 ¶¶ 6, 17 (“FAC”). The company offers technologies, devices, systems, and solutions to businesses and consumers, including external hard drives that are compatible with Apple MacBook computers. *Id.* ¶¶ 2–4, 6. Kevin Riordan, Ashley Laurent, Jeremy Bobo, and Nagui Sorial (collectively, “Plaintiffs”) are four individuals who reside in Tennessee, Minnesota, and California who had purchased and used Western Digital’s data storage devices. *Id.* ¶¶ 21, 24, 32, 35, 45, 48, 53, 56. Plaintiffs each lost data stored on these devices because of a cyber-attack. *Id.* ¶¶ 22, 33, 46, 54. Plaintiffs bring this class action against Western Digital for failure to properly secure and safeguard Plaintiffs’ and proposed class members’

Case No.: [5:21-cv-06074-EJD](#)  
ORDER GRANTING IN PART & DEN. IN PART DEF.’S MOT. TO DISMISS

1 personal, commercial, and proprietary information (“Stored Data”) within Western Digital’s data  
2 storage devices. *Id.* ¶ 2.

3 Two of Western Digital’s internet-connected devices are at issue in this action: My Book  
4 Live and My Book Duo (“Data Storage Devices” or “Covered Products”). *Id.* ¶ 4. Western  
5 Digital manufactured the Data Storage Devices in the early 2010s and has not supported them  
6 since 2015. *Id.* ¶ 90. The Data Storage Devices purportedly exhibit flaws stemming from product  
7 design and inadequate continued testing and monitoring of the devices. *Id.* ¶ 93. Plaintiffs allege  
8 that Western Digital knew of the flaws in the hardware since at least 2018. *Id.* ¶ 91.

9 On June 23, 2021, Western Digital announced that it was experiencing a cyber-attack on  
10 the Data Storage Devices. *Id.* ¶ 80. The hackers remotely executed a malicious code in the  
11 operating system of the Data Storage Devices and reset the devices’ factory settings without  
12 requiring a password. *Id.* ¶ 81. As a result, Plaintiffs’ Stored Data was wiped from Western  
13 Digital’s Data Storage Devices and users were unable to log into their devices using their own  
14 credentials. *Id.* ¶¶ 81–82. The lost data includes but is not limited to personal photos, information  
15 relating to users’ work and businesses, and financial information. *Id.* ¶ 82. Users also stored  
16 digital key data that could be used to access their digital wallets and accounts, such as  
17 cryptocurrency. *Id.* Plaintiffs are unaware of whether their Stored Data was merely wiped or  
18 whether the information is also in the hands of cyber criminals. *Id.* ¶ 100.

19 Following the cyber-attack, Western Digital announced a data recovery service program  
20 and offered to trade in affected devices for an upgraded product. *Id.* ¶ 84. To be eligible, affected  
21 users were required to contact Western Digital’s customer support center to receive a “case  
22 number” by July 31, 2021. *Id.* Data recovery operations “have mixed rates of success” and “it is  
23 highly probable that a significant portion of the lost data would be gone forever, corrupted, etc.”  
24 *Id.* ¶ 85. According to Plaintiffs, it is unlikely that Western Digital will be able to reverse the  
25 effects of the factory reset and recover the Stored Data. *Id.* ¶ 86.

26 For example, Riordan stored priceless family photos and videos on his Data Storage  
27 Device which date back to the mid-1990s that memorialize important family events and

1 milestones. *Id.* ¶ 27. Riordan contacted Western Digital’s customer support to assist with  
2 restoration of his lost data, but the attempts were unsuccessful. *Id.* ¶ 30. Riordan was able to  
3 partially recreate his photo and video library using data he had backed up on previous hard drives,  
4 but the bulk of his Stored Data (*i.e.*, hundreds of thousands of photos and videos) has been  
5 irretrievably lost. *Id.* ¶¶ 27, 31.

6 Laurent stored pictures and videos of his young son, customer contact information and  
7 correspondence of commercial value, business presentations, and personal information such as  
8 account statements, mortgage documents, tax information, and personal health information such as  
9 prescription, treatment, and diagnostic records on his Data Storage Device. *Id.* ¶¶ 38–41. His  
10 Stored Data encompassed highly sensitive information, including his social security number and  
11 information relating to his financial accounts. *Id.* ¶ 42. Laurent did not back up his Stored Data  
12 elsewhere. *Id.* ¶ 43. After the data wipe, Laurent took his Data Storage Device to Best Buy to use  
13 its data recovery services and spent \$400 attempting to recover his data. *Id.* ¶ 44. Best Buy was  
14 unable to recover his Stored Data. *Id.*

15 Bobo is self-employed and used his Data Storage Device to store business information, *i.e.*,  
16 invoices, financial statements, tax information, contracts, customer/client information and business  
17 contacts. *Id.* ¶ 51. He also stored priceless family photos. *Id.* ¶ 52. Most of his Stored Data that  
18 was lost is not backed up elsewhere. *Id.* ¶¶ 51–52.

19 Sorial used the Data Storage Device to store family photos and a wide range of personal  
20 data. *Id.* ¶ 59. The Stored Data encompassed the only copy of photos and videos from Sorial’s  
21 family, who also uploaded photos and videos to the Data Storage Device. *Id.* Their Stored Data is  
22 not uploaded elsewhere. *Id.* Sorial stored Immigration and Naturalization documents on his Data  
23 Storage Device as well as tax records and bank statements. *Id.* ¶¶ 59–60. Sorial also stored his  
24 music collection, which is primarily foreign-produced music not ordinarily available in the United  
25 States. *Id.* ¶ 61. Immediately after the data wipe, Sorial believed the issue was caused by an  
26 operator error and tried unsuccessfully to restore his data on his own. *Id.* ¶ 63. After he learned of  
27 the cyber-attack, Sorial worked with Western Digital’s customer support to restore his Stored  
28 Data, but Western Digital’s attempts were unsuccessful. *Id.* Sorial then consulted ten to fifteen

1 data recovery specialists, all of whom informed him that his data was unlikely to be recovered. *Id.*  
2 ¶ 64. The specialists informed him that even if his lost data could be recovered, any recovery  
3 would likely be in the form of raw data, meaning the data would not include file names or other  
4 organization. *Id.* The specialists quoted Sorial \$1,200 to about \$2,400 for their services. Based  
5 on this information, Sorial did not engage third party specialist services to recover his data. *Id.*

6 Plaintiffs initiated this action on behalf of themselves and a national class and California  
7 subclass of entities and persons whose Stored Data was accessed and/or deleted from their Data  
8 Storage Devices starting June 23, 2021. *Id.* ¶ 1. Plaintiffs allege five causes of action arising  
9 under the Song-Beverly Consumer Warranty Act, negligence and/or failure to warn, breach of the  
10 implied covenant of good faith and fair dealing, the UCL, and unjust enrichment. The Court  
11 granted Defendant’s first motion to dismiss with leave to amend. ECF No. 34 (“First Order”).  
12 Defendants move to dismiss the FAC under Fed. R. Civ. P. 12(b)(1) and 12(b)(6). *See generally*  
13 Mot. Plaintiffs oppose the motion. *See* ECF No. 41 (“Opp’n”).

## 14 **II. LEGAL STANDARDS**

### 15 **A. Rule 12(b)(1)**

16 Federal Rule of Procedure 12(b)(1) permits a party to assert a defense of lack of subject  
17 matter jurisdiction. Fed. R. Civ. P. 12(b)(1). A jurisdictional attack may be factual or facial.  
18 *White v. Lee*, 227 F.3d 1214, 1242 (9th Cir. 2000). A facial attack “asserts that the allegations  
19 contained in a complaint are insufficient on their face to invoke federal jurisdiction.” *Safe Air for*  
20 *Everyone v. Meyer*, 373 F.3d 1035, 1039 (9th Cir. 2004). “The district court resolves a facial  
21 attack as it would a motion to dismiss under Rule 12(b)(6): Accepting the plaintiff’s allegations as  
22 true and drawing all reasonable inferences in the plaintiff’s favor, the court determines whether the  
23 allegations are sufficient as a legal matter to invoke the court’s jurisdiction.” *Leite v. Crane Co.*,  
24 749 F.3d 1117, 1121 (9th Cir. 2014).

25 For a factual attack, defendant presents extrinsic evidence for the court’s consideration. In  
26 this case “the court need not presume the truthfulness of the plaintiff’s allegations.” *Safe Air for*  
27 *Everyone*, 373 F.3d at 1039. “When the defendant raises a factual attack, the plaintiff must

1 support her jurisdictional allegations with ‘competent proof,’ under the same evidentiary standard  
2 that governs in the summary judgment context.” *Leite*, 749 F.3d at 1121 (citations omitted).  
3 “[T]he district court is not restricted to the face of the pleadings, but may review any evidence,  
4 such as affidavits and testimony, to resolve factual disputes concerning the existence of  
5 jurisdiction.” *McCarthy v. United States*, 850 F.2d 558, 560 (9th Cir. 1988).

6 **B. Rule 12(b)(6)**

7 Rule 8(a)(2) of the Federal Rules of Civil Procedure requires a complaint to include “a  
8 short and plain statement of the claim showing that the pleader is entitled to relief.” A complaint  
9 that fails to meet this standard may be dismissed pursuant to Rule 12(b)(6). Rule 8(a) requires a  
10 plaintiff to plead “enough facts to state a claim to relief that is plausible on its face.” *Bell Atl.*  
11 *Corp. v. Twombly*, 550 U.S. 544, 570 (2007). “A claim has facial plausibility when the plaintiff  
12 pleads factual content that allows the court to draw the reasonable inference that the defendant is  
13 liable for the misconduct alleged.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). While plaintiffs  
14 must allege “more than a sheer possibility that a defendant has acted unlawfully,” the plausibility  
15 standard “is not akin to a probability requirement.” *Id.*

16 For purposes of ruling on a Rule 12(b)(6) motion, the Court generally “accept[s] factual  
17 allegations in the complaint as true and construe[s] the pleadings in the light most favorable to the  
18 nonmoving party.” *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir.  
19 2008). The Court need not, however, “assume the truth of legal conclusions merely because they  
20 are cast in the form of factual allegations.” *Fayer v. Vaughn*, 649 F.3d 1061, 1064 (9th Cir. 2011)  
21 (per curiam). Mere “conclusory allegations of law and unwarranted inferences are insufficient to  
22 defeat a motion to dismiss.” *Adams v. Johnson*, 355 F.3d 1179, 1183 (9th Cir. 2004). The Court  
23 may also “look beyond the plaintiff’s complaint to matters of public record” without converting  
24 the Rule 12(b)(6) motion into a motion for summary judgment. *Shaw v. Hahn*, 56 F.3d 1128,  
25 1129 (9th Cir. 1995).

26 **III. DISCUSSION**

27 Defendant argues that Plaintiffs lack Article III standing over claims based on future data

1 misappropriation, prayers for injunctive relief, and putative nationwide class claims, and that  
2 Plaintiffs’ claims must be dismissed under Federal Rule of Civil Procedure 12(b)(1). In the  
3 alternative, Defendant argues that this action must be dismissed under Federal Rule of Civil  
4 Procedure 12(b)(6) because the Complaint fails to state a claim for which relief can be granted.  
5 The Court addresses each argument in turn.

6 **A. Standing**

7 To confer standing, a plaintiff must establish three elements: (i) plaintiff suffered an injury  
8 in fact; (ii) there is a causal connection between the defendant’s conduct and the alleged injury;  
9 and (iii) the injury is redressable by a favorable decision. *Lujan v. Defs. of Wildlife*, 504 U.S. 555,  
10 560 (1992).

11 **1. Claims Based on Future Data Misuse<sup>1</sup>**

12 Defendant facially challenges the Court’s subject matter jurisdiction over Plaintiffs’ claims  
13 to the extent they are based on a theory of injury or seek relief for future data misuse. Strictly  
14 facial challenges to subject matter jurisdiction are treated as “any other motion to dismiss on the  
15 pleadings for lack of jurisdiction,” and therefore the court must “determine whether the complaint  
16 alleges ‘sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its  
17 face.’” *Terenkian v. Republic of Iraq*, 694 F.3d 1122, 1131 (9th Cir. 2012) (quoting *Ashcroft v.*  
18 *Iqbal*, 556 U.S. 662, 678 (2009)) (quotations and citation omitted).

19 According to Western Digital, Plaintiffs’ theory that they face a risk of future data misuse  
20 is based on a hypothetical injury. Mot. at 5. “To establish injury in fact, a plaintiff must show that  
21 he or she suffered ‘an invasion of a legally protected interest’ that is ‘concrete and particularized’  
22 and ‘actual or imminent, not conjectural or hypothetical.’” *Spokeo, Inc. v. Robins*, 578 U.S. 330,  
23

---

24 <sup>1</sup> Plaintiffs allege two theories of injury: (1) they lost data stored on the My Book Live device as a  
25 result of the factory reset, and (2) they face a risk of future data misuse “if [their personal data] has  
26 made its way into the hands of cyber-criminals.” FAC ¶ 100. In the First Order, the Court found  
27 that Plaintiffs lacked standing under either theory. See First Order at 7. Plaintiffs have amended  
28 the FAC to include detailed allegations showing concrete and particularized harm with respect to  
the four representative plaintiffs by alleging that the permanent loss of their stored data caused  
them to suffer an injury in fact. Western Digital does not challenge Plaintiffs’ loss of data injury.

1 339 (2016) (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992)). The “risk of real  
2 harm” can satisfy the requirement of concreteness. *Spokeo*, 578 U.S. at 341. A plaintiff alleging a  
3 risk of future harm satisfies the injury in fact requirement where he or she faces a “credible threat  
4 of harm” that is “both real and immediate” and “not conjectural or hypothetical.” *Krottner v.*  
5 *Starbucks Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010).

6 The First Order found that Plaintiffs failed to plead any facts to support a risk of future  
7 data misuse, and unsupported speculative allegations of future harm do not establish an injury in  
8 fact. First Order at 5–6. Plaintiffs amended their complaint to include allegations that Laurent and  
9 Sorial stored sensitive personal information on their Data Storage Devices, including social  
10 security numbers, naturalization documents, and financial account information, which was wiped  
11 from their Data Storage Devices by cyber criminals during the hack. *Id.* ¶¶ 41, 51, 60. Plaintiffs  
12 allege that if cyber criminals gained access to Plaintiffs and Class Members’ Stored Data during  
13 the hack, it could be used “to perpetrate a variety of crimes that harm victims” such as identity  
14 theft and immigration fraud. *Id.* ¶¶ 101, 107.

15 Plaintiffs rely on *Zappos* to argue the fact that the hackers accessed personal information  
16 that could be used to commit a crime establishes a “substantial risk” that the hackers *will* commit  
17 identity theft or fraud. *In re Zappos.com, Inc.*, 888 F.3d 1020, 1029 (9th Cir. 2018). In *Zappos*,  
18 plaintiffs’ personal data was accessed during a breach of Zappos.com’s servers where hackers  
19 allegedly stole the names, account numbers, passwords, contact information, and credit and debit  
20 card information of approximately 24 million Zappos customers. *Id.* at 1023. Some plaintiffs  
21 alleged that the hackers used stolen information about them to conduct subsequent financial  
22 transactions resulting in financial losses while other plaintiffs alleged that the Zappos data breach  
23 put them at “imminent risk” of identity theft. *Id.* The district court dismissed the claims of the  
24 plaintiffs who alleged that the Zappos data breach put them at risk of identity theft for lack of  
25 Article III standing. *Id.* These plaintiffs appealed. *Id.* The Ninth Circuit reversed, holding that  
26 the appellees sufficiently alleged standing based on the risk of identity theft. *Id.*

27 *Zappos* is distinguishable from the present action. In *Zappos*, plaintiffs alleged that

1 hackers stole their data. *Id.* at 1027 n.7 (noting that the complaint included emails sent to Zappos  
2 from other customers saying that their credit cards were fraudulently used following the breach).  
3 The Ninth Circuit reasoned that the “sensitivity of the personal information, *combined with its*  
4 *theft*, led us to conclude that the plaintiffs had adequately alleged an injury in fact supporting  
5 standing.” *Id.* (emphasis added). Here, Plaintiffs *speculate* that their lost data may have “made its  
6 way into the hands of cyber criminals. FAC ¶ 100 (“Plaintiffs and Class Members are unaware as  
7 to whether their Stored Data was merely deleted, or if such information has made its way into the  
8 hands of cyber-criminals.”). The *Zappos* court noted that several allegations lent support to  
9 appellees’ assertion that the information stolen by the hackers could be used to commit identity  
10 fraud or theft in the future, including: (1) allegations of the plaintiffs “who alleged that the hackers  
11 had already commandeered their accounts or identities using information taken from Zappos” had  
12 suffered financial losses as a result, and (2) allegations of two appellees that “the hackers took  
13 over their AOL accounts and sent advertisements to people in their address books.” *In re*  
14 *Zappos.com, Inc.*, 888 F.3d at 1027–28. Here, the FAC is devoid of any allegations indicating  
15 data theft. *See e.g., Foster v. Essex Prop. Trust, Inc.*, 2015 WL 7566811, at \*3 (N.D. Cal. Nov.  
16 25, 2015) (“Since Plaintiffs have not shown, . . . that any of their information was actually stolen,  
17 their theory of future harm is implausible.”); *Stasi v. Inmediata Health Grp. Corp.*, No. 19-CV-  
18 2353 JM (LL), 2020 WL 2126317, at \*6 (S.D. Cal. May 5, 2020) (distinguishing *Zappos* based on  
19 plaintiffs failure to allege “their information was stolen or hacked” and noting that plaintiffs  
20 instead allege “that their information was temporarily accessible via the internet, but not  
21 necessarily copied or even viewed by a potential identity thief”); *see also Burns v. Mammoth*  
22 *Media, Inc.*, No. 2-CV-004855-DDP-SKX, 2023 WL 5608389, at \*3 (C.D. Cal. Aug. 29, 2023)  
23 (noting that *Zappos* does not suggest that a hacked account on its own “evidence[s] an ongoing  
24 risk of identity theft or constitute[s] an injury in fact”). Instead, Plaintiffs rely on mere speculation  
25 and conjecture that their data may have been stolen.

26 For these reasons, Plaintiffs have not sufficiently alleged an injury in fact as to their claims  
27 based on future data misuse. Because Plaintiffs have failed to establish a risk of future injury, they



1 have not pled any allegations that could support their claims for injunctive relief and therefore lack  
2 standing to pursue such claims. *See Summers v. Earth Island Inst.*, 555 U.S. 488, 493 (2009); *see*  
3 *also DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 352 (2006) (“[A] plaintiff must demonstrate  
4 standing for each claim he seeks to press.”). Accordingly, the Court dismisses Plaintiffs’ claims  
5 for injunctive relief.

6 **2. Standing to Allege a Nationwide Class**

7 Plaintiffs are California, Tennessee, and Minnesota citizens alleging violations of  
8 California’s Song-Beverly Consumer Warranty Act (the “Song-Beverly Act”) and UCL on behalf  
9 of a California subclass. Plaintiffs’ also assert negligence/failure to warn, breach of the implied  
10 covenant of good faith and fair dealing, and unjust enrichment claims on behalf of the nationwide  
11 class.<sup>2</sup> Plaintiffs do not specify which state law or laws they intend to assert in their common law  
12 causes of action. Western Digital therefore asks the Court to dismiss all putative claims on behalf  
13 of a nationwide class because Plaintiffs do not have standing to assert claims under the laws of  
14 states in which they do not live, *i.e.*, they can only assert claims under California, Tennessee, and  
15 Minnesota law. Mot. at 7.

16 A district court may address Article III standing to bring nationwide-class allegations at the  
17 pleading stage. *See Drake v. Toyota Motor Corp.*, No. 2:20-CV-01421-SB-PLA, 2020 WL  
18 7040125, at \*3 (C.D. Cal. Nov. 23, 2020) (collecting cases). The issue may be properly addressed  
19 prior to class certification “when a plaintiff’s lack of standing is ‘plain enough from the  
20 pleadings,’ it can form appropriate grounds for dismissal even if it overlaps with issues regarding  
21 whether the named plaintiffs are adequate representatives under Rule 23.” *Carpenter v. PetSmart,*  
22 *Inc.*, 441 F. Supp. 3d 1028, 1039 (S.D. Cal. 2020) (quoting *Broomfield v. Craft Brew All., Inc.*,  
23 No. 17-cv-01027-BLF, 2017 WL 3838453, at \*14 (N.D. Cal. Sept. 1, 2017)). However,  
24 California district courts typically decline to rule on nationwide class claims arising under  
25

26 \_\_\_\_\_  
27 <sup>2</sup> Plaintiffs initially asserted a cause of action for violation of the Magnuson-Moss Warranty Act,  
28 15 U.S.C. § 2301, *et seq.*, but have since removed this claim from the FAC.

1 California consumer protection statutes at the pleading stage “based on the need to conduct a case-  
2 specific choice of law analysis.” *Czuchaj v. Conair Corp.*, 2014 U.S. Dist. LEXIS 54410, \*24  
3 (S.D. Cal. April 16, 2014); *see also Won Kyung Hwang v. Ohso Clean, Inc.*, 2013 U.S. Dist.  
4 LEXIS 54002, \*59 (N.D. Cal. April 16, 2013) (choice of law questions are premature at the  
5 pleading stage).

6 The Court declines to engage in a choice of law analysis at the pleading stage, particularly  
7 where it lacks sufficient briefing to engage in detailed analysis. *See Czuchaj*, 2014 U.S. Dist.  
8 LEXIS 54410, \*25; *see also Cooper v. Tokyo Elec. Power Co. Holdings*, 960 F.3d 549, 559 (9th  
9 Cir. 2020). This inquiry is most appropriately addressed at class certification.

10 **B. Sufficiency of the Allegations**

11 **1. Song-Beverly Act Claim**

12 Western Digital alleges that Plaintiffs fail to state a claim under the Song-Beverly Act.  
13 Mot. at 13. “Under the Song-Beverly Act, every retail sale of ‘consumer goods’ in California  
14 includes an implied warranty by the manufacturer and the retail seller that the goods are  
15 ‘merchantable.’” *Mexia v. Rinker Boat Co., Inc.*, 174 Cal. App. 4th 1297, 1303 (2009) (quoting  
16 Cal. Civ. Code, §§ 1791.3, 1792). Merchantability refers to whether the goods:

- 17 (1) Pass without objection in the trade under the contract description.  
18 (2) Are fit for the ordinary purposes for which such goods are used.  
19 (3) Are adequately contained, packaged, and labeled.  
20 (4) Conform to the promises or affirmations of fact made on the  
container or label.

21 Cal. Civ. Code § 1791.1.

22 First, Western Digital contends that this claim is deficient because Plaintiffs fail to allege  
23 whether they purchased the Data Storage Devices in California. Mot. at 9–10. The Court agrees.  
24 None of the representative plaintiffs are alleged to have purchased their devices in California.  
25 Indeed, the implied warranty of merchantability attaches to “every sale of consumer goods that are  
26 sold at retail *in this state*.” Cal. Civ. Code § 1792; *see In re Nexus 6P Prod. Liab. Litig.*, 293 F.  
27 Supp. 3d 888, 948 (N.D. Cal. 2018) (dismissing Song-Beverly Act claim for failure to allege  
whether the phones were purchased in California). Plaintiffs contend that, in drawing all

1 reasonable inferences in their favor, the Court should infer that Plaintiffs Bobo and Sorial  
2 purchased their devices in California simply because the FAC alleges they are California residents.  
3 Opp’n at 10. However, it is well established that courts “may not supply essential elements of the  
4 claim that were not initially pled.” *Chapman v. Pier 1 Imps. (U.S.), Inc.*, 631 F.3d 939, 954 (9th  
5 Cir. 2011) (quoting *Pena v. Gardner*, 976 F.2d 469, 471 (9th Cir. 1992)).

6 Second, Western Digital alleges the Song-Beverly Act claim is barred by the statute of  
7 limitations. Mot. at 10. The Song-Beverly Act does not have its own statute of limitations.  
8 *Mexia*, 174 Cal. App. 4th at 1305. Instead, it is governed by Section 2725 of the Uniform  
9 Commercial Code. *MacDonald v. Ford Motor Co.*, 37 F. Supp. 3d 1087, 1100 (N.D. Cal. 2014).  
10 Section 2725 provides that “[a]n action for breach of any contract for sale must be commenced  
11 within four years after the cause of action has accrued.” Cal. Com. Code § 2725(1). “A cause of  
12 action accrues when the breach occurs, regardless of the aggrieved party’s lack of knowledge of  
13 the breach.” Cal. Com. Code § 2725(2). Here, Plaintiffs do not allege when they purchased their  
14 Data Storage Devices. Western Digital challenges whether Plaintiffs’ claims fall outside the four-  
15 year limitations period since the allegations indicate that Western Digital ended support for the  
16 devices at issue in 2015. Mot. at 10–11.

17 Accordingly, the Court GRANTS Western Digital’s motion to dismiss the Song-Beverly  
18 Act claim with leave to amend to assert where and when the devices were purchased.

19 **2. Failure to Warn Claim**

20 Plaintiffs’ second cause of action asserts a claim for negligent failure to warn.  
21 “Negligence law in a failure-to-warn case requires a plaintiff to prove that a manufacturer or  
22 distributor did not warn of a particular risk for reasons which fell below the acceptable standard of  
23 care, *i.e.*, *what a reasonably prudent manufacturer would have known and warned about.*” *Rosa v.*  
24 *City of Seaside*, 675 F. Supp. 2d 1006, 1014 (N.D. Cal. 2009), *aff’d sub nom. Rosa v. Taser Int’l,*  
25 *Inc.*, 684 F.3d 941 (9th Cir. 2012) (emphasis in original) (quotations and citations omitted). At the  
26 pleading stage, “a plaintiff must allege, at a minimum, that a defect in the product caused the  
27 plaintiff’s injury and that ‘the defect in the product was due to the negligence of the defendant.’”

1 *Mountain Club Owner’s Ass’n v. Graybar Elec. Co.*, No. CIV. 2:13-1835 WBS K, 2014 WL  
2 130767, at \*2 (E.D. Cal. Jan. 14, 2014) (quoting *Merrill v. Navegar, Inc.*, 26 Cal.4th 465, 479  
3 (2001)). “A bare allegation that defendants were negligent in their design is an insufficient legal  
4 conclusion.” *Fontalvo v. Sikorsky Aircraft Corp.*, CIV. NO. 13–331 GPC KSC, 2013 WL  
5 4401437, at \*5 (S.D. Cal. Aug.15, 2013).

6 Here, Plaintiffs allege that Western Digital breached its general duty of care to Plaintiffs in  
7 failing to adequately warn them of the risks of the Data Storage Devices, “including the legitimate  
8 threat of cyber-attack, and in failing to comply with applicable industry standards, and state and  
9 federal laws, rules, regulations and standards.” FAC ¶¶ 130–31. Western Digital asserts that  
10 Plaintiffs failure to warn claim should be dismissed because Plaintiffs fail to plausibly allege that  
11 Western Digital knew or should have known of any danger of cyber-attack or that the alleged  
12 failure to warn caused Plaintiffs’ harm. Mot. at 11–12.

13 The FAC purportedly identifies one defect in the Data Storage Devices—a “flaw” in  
14 Western Digital’s My Cloud device system. FAC ¶ 87. In support, Plaintiffs cite one report  
15 finding “a pair of hacking researchers searching for exploits in various technology systems”  
16 identified a “vulnerability” in Western Digital’s My Cloud OS 3 system published in February  
17 2021. FAC ¶ 87. However, Plaintiffs fail to explain in sufficient detail exactly what this “flaw” is  
18 or how it falls below the applicable standard of care. Indeed, “[a] claim of negligent failure to  
19 warn necessarily implicates a defective product or a product rendered defective.” *Sapiro v.*  
20 *Encompass Ins.*, No. C 03-4587 MHP, 2004 WL 2496090, at \*6 (N.D. Cal. Nov. 2, 2004).

21 The remainder of the allegations conclusively state that Western digital knew or should  
22 have known that its Data Storage Devices were vulnerable to attacks by hackers. For example,  
23 Plaintiffs allege that Western Digital “allowed inherent flaws in the WD My Book Live and My  
24 Book Duo to remain within those systems and left Representative Plaintiffs and Class Members  
25 unprotected against a cyber-attack,” FAC ¶ 88, however, Plaintiffs fail to identify any specific  
26 flaw in Western Digital’s Data Storage Device. Plaintiffs also allege that the company “has a  
27 history of allowing inherent flaws in the Covered Products that were dangerous to customers’

1 information,” but fails to allege any specific instances showing that Western Digital “failed both to  
2 take action to protect customers’ data and to adequately address and warn consumers of  
3 Defendant’s resultant security concerns.” *Id.* ¶ 89. Without providing any support for this  
4 allegation, the Court cannot assume Digital Western has a “history” of flaws in its devices.

5 In sum, the FAC is devoid of allegations specifying what the vulnerability is in the Data  
6 Storage Device and how it enabled a cyber-attack. Without these allegations the Court cannot  
7 properly assess whether Western Digital failed to warn Plaintiffs. Thus, Plaintiffs have failed to  
8 state a cognizable claim for negligent failure to warn. The Court GRANTS Western Digital’s  
9 motion to dismiss with respect to this claim with leave to amend.

10 **3. Implied Covenant of Good Faith and Fair Dealing Claim**

11 Plaintiffs’ third cause of action alleges that Digital Western breached the implied covenant  
12 of good faith and fair dealing.

13 “Every contract imposes upon each party a duty of good faith and fair dealing in its  
14 performance and its enforcement.” *Carma Developers, Inc. v. Marathon Dev. Cal., Inc.*, 2 Cal.  
15 4th 342, 371 (1992) (quotations omitted). Under California law, to establish a breach of the  
16 covenant of good faith and fair dealing a plaintiff must plead that: “(1) the parties entered into a  
17 contract; (2) the plaintiff fulfilled his obligations under the contract; (3) any conditions precedent  
18 to the defendant’s performance occurred; (4) the defendant unfairly interfered with the plaintiff’s  
19 rights to receive the benefits of the contract; and (5) the plaintiff was harmed by the defendant’s  
20 conduct.” *Rosenfeld v. JPMorgan Chase Bank, N.A.*, 732 F. Supp. 2d 952, 968 (N.D. Cal. 2010).

21 "In addition, the implied covenant “cannot impose substantive duties or limits on the contracting  
22 parties beyond those incorporated in the specific terms of their agreement.” *Agosta v. Astor*, 120  
23 Cal.App.4th 596, 607, 15 Cal.Rptr.3d 565 (2004) (internal citation omitted).

24 Western Digital contends that Plaintiffs have failed to identify any express contractual term  
25 from which this duty arises. Mot. at 13. While a “breach of a specific provision of the contract is  
26 not a necessary prerequisite to establishing a breach of the implied covenant of good faith and fair  
27 dealing,” a plaintiff must allege an express term “on which to hinge an implied duty.” *In re*

1 *Facebook PPC Advert. Litig.*, 709 F. Supp. 2d 762, 769 (N.D. Cal. 2010) (quotations and citations  
2 omitted). Plaintiffs maintain there is a contract because “Plaintiffs purchased and owned Western  
3 hard drives.” Opp’n at 13. Plaintiffs allege that they purchased the Data Storage Devices “in  
4 reliance on Defendant’s representation that they were secure and that Defendant was committed to  
5 safely preserving their data.” FAC ¶ 8. Digital Western allegedly breached the implied covenant  
6 of good faith and fair dealing “by failing to inform Representative Plaintiffs and Class Members of  
7 the defects and/or vulnerabilities inherent in the Covered Products and failing to properly repair  
8 and/or provide a patch for those defects and/or vulnerabilities.” FAC ¶ 137.

9 However, Plaintiffs do not specify whether the Data Storage Devices were purchased from  
10 Western Digital such that the Court can infer a valid contract exists between the parties. *Guz v.*  
11 *Bechtel Nat’l, Inc.*, 24 Cal.4th 317, 375, 100 Cal.Rptr.2d 352, 8 P.3d 1089 (2000) (holding that  
12 breach of the implied covenant of good faith and fair dealing claim is predicated on the existence  
13 of a contract). As pled, the FAC lacks sufficient allegations to establish the existence of a contract  
14 from which an implied covenant of good faith and fair dealing may arise.

15 Accordingly, Plaintiffs’ claim for breach of the implied covenant of good faith and fair  
16 dealing is dismissed with leave to amend.

17 **4. UCL Claim**

18 Next, Western Digital argues that Plaintiffs’ fourth cause of action arising under  
19 California’s Unfair Competition Law (“UCL”) fails as a matter of law. Mot. at 15.

20 The UCL prohibits “any unlawful, unfair or fraudulent business act.” Cal. Bus. & Prof.  
21 Code § 17200. Courts interpret the UCL as establishing three distinct “prongs” of liability for  
22 business practices that are (1) unlawful, (2) unfair, or (3) fraudulent. *Hadley v. Kellogg Sales Co.*,  
23 243 F. Supp. 3d 1074, 1089 (N.D. Cal. 2017). Plaintiffs assert causes of action under all three  
24 prongs. Plaintiffs bring the UCL claim on behalf of the putative California subclass based on the  
25 following alleged unlawful business practices: Western Digital’s “sub-standard design” of the  
26 Data Storage Devices, failure to warn of the risks of continued use of the device, failure to provide  
27 a “patch” for defects, failure to recall the products, “and/or Defendant’s deceptive

1 misrepresentations, concealments and suppressions of material fact.” FAC ¶¶ 140, 144.

2 As a threshold matter, Western Digital challenges whether Plaintiffs can show they have an  
3 adequate remedy at law. Mot. at 15. Plaintiffs request an injunction, restitution damages, and/or  
4 other equitable relief including disgorgement or ill-gotten gains, refunds, interest, and reasonable  
5 attorneys’ fees. FAC ¶ 150. Western Digital contends that *Sonner v. Premier Nutrition Corp.*  
6 forecloses Plaintiffs’ UCL claim. 971 F.3d 834 (9th Cir. 2020).

7 In *Sonner*, the district court dismissed a plaintiff’s UCL claim because she had “failed to  
8 establish that she lacked an adequate legal remedy” given that she had previously sought damages  
9 under another statute for the same conduct and the UCL is subject to California’s inadequate-  
10 remedy-at-law doctrine. *Id.* at 838. The Ninth Circuit affirmed the district court, noting that a  
11 plaintiff “must establish that she lacks an adequate remedy at law before securing equitable  
12 restitution for past harm under the UCL and CLRA.” *Id.* at 844. Here, the fact that the FAC fails  
13 to allege that Plaintiffs lack an adequate remedy of law is fatal to Plaintiffs’ claims for equitable  
14 restitution under the UCL. *Id.* (citing *O’Shea v. Littleton*, 414 U.S. 488, 502 (1974)). Although  
15 Plaintiffs suggest in opposition that their requested remedies are inadequate or incomplete  
16 compensation for Plaintiffs’ harm, the FAC is devoid of any such allegations. *See In re California*  
17 *Gasoline Spot Mkt. Antitrust Litig.*, No. 20-CV-03131-JSC, 2021 WL 1176645, at \*8 (N.D. Cal.  
18 Mar. 29, 2021) (collecting cases).

19 Plaintiffs UCL is therefore dismissed with leave to amend to the extent Plaintiffs can  
20 allege that they lack an adequate remedy of law.

### 21 5. Unjust Enrichment Claim

22 Finally, Western Digital asserts that Plaintiffs’ fifth claim for unjust enrichment fails  
23 because it is not a standalone cause of action. Mot. at 23.

24 Although there is no standalone cause of action for unjust enrichment under California  
25 law, “[w]hen a plaintiff alleges unjust enrichment, a court may ‘construe the cause of action as a  
26 quasi-contract claim seeking restitution.’” *Astiana v. Hain Celestial Grp., Inc.*, 783 F.3d 753, 762  
27 (9th Cir. 2015) (quoting *Rutherford Holdings, LLC v. Plaza Del Rey*, 223 Cal. App. 4th 221, 231

1 (2014)). Here, Plaintiffs allege that Western Digital obtained a benefit by failing to disclose the  
2 fact that the Data Storage Device is defective before Plaintiffs purchased and used the product.  
3 FAC ¶¶ 152, 155. Western Digital was “unjustly enriched at the expense of Representative  
4 plaintiffs and Class Members.” *Id.* ¶ 156. Plaintiffs seek an order from the Court “requiring  
5 Defendant to refund, disgorge, and pay as restitution any profits, benefits, and other compensation  
6 obtained by Defendant.” *Id.* ¶ 158. The Court construes these allegations as pleading a claim for  
7 quasi-contract seeking restitution and, therefore, Plaintiffs’ unjust enrichment claim is not subject  
8 to dismissal on the basis that it is improperly pled as a standalone claim. *See Rabin v. Google*  
9 *LLC*, No. 22-CV-04547-BLF, 2023 WL 4053804, at \*12 (N.D. Cal. June 15, 2023).

10 Western Digital also contends that, should the Court construe Plaintiffs’ claim as a quasi-  
11 contract cause of action, Plaintiffs’ claim should still be dismissed because Plaintiffs allege the  
12 existence of a valid contract between the parties “covering the same subject matter” but have  
13 failed to allege facts showing that the contract is unenforceable. Mot. at 23 (quoting *Saroya v.*  
14 *Univ. of the Pac.*, No. 5:20-cv-03196-EJD, 2021 WL 2400986, at \*3 (N.D. Cal. June 11, 2021)).  
15 Plaintiffs assert that they may plead quasi-contract damages in the alternative. Opp’n at 17. The  
16 Court agrees. At the pleading stage plaintiffs may allege inconsistent remedies of recovery in the  
17 alternative. *Aberin v. Am. Honda Motor Co., Inc.*, No. 16-CV-04384-JST, 2018 WL 1473085, at  
18 \*9 (N.D. Cal. Mar. 26, 2018). It is well established that “claims for restitution or unjust  
19 enrichment may survive the pleading stage when pled as an alternative avenue of relief, though the  
20 claims, as alternatives, may not afford relief if other claims do.” *Colucci v. ZonePerfect Nutrition*  
21 *Co.*, No. 12-2907-SC, 2012 WL 6737800, at \*10 (N.D. Cal. Dec. 28, 2012) (collecting cases).

22 Accordingly, the Court declines to dismiss Plaintiffs’ alternative claim for restitution based  
23 on quasi-contract.

24 **IV. CONCLUSION**

25 For the foregoing reasons, Western Digital’s motion to dismiss is GRANTED IN PART  
26 and DENIED IN PART. In sum, the Court:

- 27 1) GRANTS Defendant’s motion to dismiss Plaintiffs’ claims based on future data misuse



- 1 and therefore dismisses Plaintiffs' claims for injunctive relief;
- 2 2) DENIES Defendant's motion to dismiss Plaintiffs' nationwide-class allegations for
- 3 lack of standing;
- 4 3) GRANTS Defendant's motion to dismiss the Song-Beverly Act claim;
- 5 4) GRANTS Defendant's motion to dismiss the failure to warn claim;
- 6 5) GRANTS Defendant's motion to dismiss the UCL claim;
- 7 6) GRANTS Defendant's motion to dismiss the breach of the implied covenant of good
- 8 faith and fair dealing claim; and
- 9 7) DENIES Defendant's motion to dismiss Plaintiffs' claim for unjust enrichment.

10 Plaintiffs request leave to amend any pleading deficiencies. When dismissing a complaint

11 for failure to state a claim, a court should grant leave to amend "unless it determines that the

12 pleading could not possibly be cured by the allegation of other facts." *Lopez v. Smith*, 203 F.3d

13 1122, 1127 (9th Cir. 2000). The Court finds that amendment would not be futile. Accordingly,

14 the Court grants Defendant's motion to dismiss with leave to amend. Should Plaintiffs choose to

15 file an amended complaint, they must do so by **October 16, 2023**. Failure to cure the deficiencies

16 identified in this Order will result in dismissal of those claims.

17 Plaintiffs may not add new claims or parties without leave of the Court or stipulation by

18 the parties pursuant to Federal Rule of Civil Procedure 15.

19 **IT IS SO ORDERED.**

20 Dated: September 29, 2023

21 

22 EDWARD J. DAVILA  
23 United States District Judge