

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 MOTION TO DISMISS**  
Re: Dkt. No. 22

Plaintiffs Kevin Riordan, Ashley Laurent, Jeremy Bobo, and Nagui Sorial bring claims for injunctive and monetary relief for harm arising out of a data breach. *See* Plaintiffs’ Complaint for Damages, Injunctive and Equitable Relief (“*Compl.*”), Dkt. No. 1. Defendant Western Digital Corporation moves to dismiss Plaintiffs’ Complaint. *See* Defendant Western Digital Corporation’s Motion to Dismiss Plaintiffs’ Complaint (“*Mot.*”), Dkt. No. 22. On October 21, 2021, Plaintiffs filed an opposition, to which Defendant filed a reply. *See* Plaintiffs’ Opposition to Defendant’s Motion to Dismiss Plaintiffs’ Complaint (“*Opp.*”), Dkt. No. 24; Defendant’s Reply in Support of Motion to Dismiss Plaintiffs’ Complaint (“*Reply*”), Dkt. No. 25. Having considered the record in this case, the Parties’ papers, and the relevant law, the Court **GRANTS** Defendant’s motion to dismiss.<sup>1</sup>

**I. BACKGROUND**

Defendant Western Digital is a leading global and data storage brand that offers technologies, devices, systems, and solutions to businesses and consumers. *Compl.* ¶ 46. On June

---

<sup>1</sup> On May 27, 2022, the Court found this motion appropriate for decision without oral argument pursuant to Civil Local Rule 7-1(b). *See* Dkt. No. 33.  
Case No.: [5:21-cv-06074-EJD](#)  
**ORDER GRANTING MOTION TO DISMISS**

1 23, 2021, Defendant announced that two of its legacy Internet-connected hard drives, My Book  
2 Live and My Book Live Duo (the “Covered Products”), had been attacked by third-party hackers.  
3 Compl. ¶ 58. The hackers accessed the Covered Products through vulnerabilities that allowed  
4 them to execute malicious code in the storage devices’ operating systems and initiate a factory  
5 reset. Compl. ¶ 59. Through the factory reset, the hackers remotely erased data stored on certain  
6 Covered Products. Compl. ¶ 4. Specifically, Plaintiffs allege that the Covered Products had  
7 “multiple security flaws present in their software from their creation that allowed remote hackers  
8 to remove customer data thereon and perform a ‘factory reset’ of the devices without the  
9 customers’ login information.” Compl. ¶ 8.

10 Plaintiffs purchased the Covered Products “in reliance on [Defendant’s] representation that  
11 [the products] were secure, and that [Defendant] was committed to safely preserving their data.”  
12 Compl. ¶ 8. As a result of Defendant’s failure to meet this expectation, Plaintiffs contend that  
13 they have “suffered damages, including but not limited to years-worth of lost sensitive, intimate,  
14 and valuable personal, commercial and/or proprietary information (the ‘Stored Data’).” Compl.  
15 ¶ 5. The nature of the Stored Data ranges from “important financial information to priceless  
16 personal items such as family photos of vacations, childbirths, graduations and holidays.” Compl.  
17 ¶ 5. Plaintiffs allege that they stored massive amounts of data on the Covered Products, all of  
18 which has been deleted. In many instances, Plaintiffs “kept little or no inventory of what  
19 information was stored on their Covered Products, meaning that the full extent of their loss may  
20 never be fully known.” Compl. ¶ 7. Plaintiffs worry that their private information is being used  
21 by cyber criminals. Compl. ¶ 94.

22 The My Book Live and My Book Live Duo devices were manufactured by Western Digital  
23 in the early 2010s. However, the Covered Products have not been supported by Western Digital  
24 since 2015. Compl. ¶ 68. Following the attack, Defendant offered affected users access to a free  
25 data recovery service program and the option to trade in impacted devices for upgraded products.  
26 Compl. ¶ 62. Affected users were instructed to contact Western Digital’s support center by July  
27 31, 2021, to participate in these programs. Compl. ¶ 62. Plaintiffs do not allege that they

1 participated in the data recovery or trade-in programs that Defendant offered. However, Plaintiffs  
2 do allege that “such data recovery operations traditionally have mixed rates of success.” Compl.  
3 ¶ 63. Plaintiffs speculate that even if “some data might be recovered,” “it is highly probable that a  
4 significant portion . . . would be gone forever” or “corrupted.” Compl. ¶ 63.

5 Plaintiffs argue that Defendant had a “duty to design and provide products that would not  
6 jeopardize [Plaintiffs’] Stored Data” and that Defendant “breached this duty by allowing known  
7 issues and/or vulnerabilities with the products to remain without any remedy or notification—  
8 issues and abilities that were ultimately used by cyber-criminals to access and/or delete massive  
9 volumes of Class Member data.” Compl. ¶ 8. Based on these allegations, Plaintiffs bring claims  
10 for: (1) violation of the Song-Beverly Consumer Warranty Act (the “SBA”), Cal. Civ. Code  
11 § 1792, *et seq.*; (2) violation of the Magnuson-Moss Warranty Act (the “MMWA”), 15 U.S.C.  
12 § 2301, *et seq.*; (3) negligence/failure to warn; (4) breach of the covenant of good faith and fair  
13 dealing; (5) unfair business practices (“UCL”), Cal. Bus. & Prof. Code § 17200, *et seq.*; and (6)  
14 unjust enrichment. Defendant argues that Plaintiffs’ claims must be dismissed under either  
15 Federal Rule of Civil Procedure 12(b)(1) or Federal Rule of Civil Procedure 12(b)(6).

16 **II. LEGAL STANDARD**

17 A motion to dismiss under Rule 12(b)(1) is a challenge to the court’s subject matter  
18 jurisdiction. The party mounting a Rule 12(b)(1) challenge may bring a facial challenge and show  
19 that the on the face of the pleadings, the court lacks jurisdiction, or may present extrinsic evidence  
20 for the Court’s consideration. *See White v. Lee*, 227 F.3d 1214, 1242 (9th Cir. 2000) (“Rule  
21 12(b)(1) jurisdictional attacks can be either facial or factual”). “In a facial attack, the challenger  
22 asserts that the allegations contained in a complaint are insufficient on their face to invoke federal  
23 jurisdiction.” *Safe Air for Everyone v. Meyer*, 373 F.3d 1035, 1039 (9th Cir. 2004).

24 In ruling on a Rule 12(b)(1) motion attacking the complaint on its face, the Court accepts  
25 the allegations of the complaint as true. *See, e.g., Wolfe v. Strankman*, 392 F.3d 358, 362 (9th Cir.  
26 2004). “By contrast, in a factual attack, the challenger disputes the truth of the allegations that, by  
27 themselves, would otherwise invoke federal jurisdiction.” *Safe Air*, 373 F.3d at 1039.

1           “With a factual Rule 12(b)(1) attack . . . a court may look beyond the complaint to matters  
2 of public record without having to convert the motion into one for summary judgment. It also  
3 need not presume the truthfulness of the plaintiff[’s] allegations.” *White*, 227 F.3d at 1242  
4 (internal citation omitted); *see also Thornhill Pub. Co., Inc. v. Gen. Tel. & Elecs. Corp.*, 594 F.2d  
5 730, 733 (9th Cir. 1979) (“Where the jurisdictional issue is separable from the merits of the case,  
6 the judge may consider the evidence presented with respect to the jurisdictional issue and rule on  
7 that issue, resolving factual disputes if necessary . . . ‘[N]o presumptive truthfulness attaches to  
8 plaintiff’s allegations, and the existence of disputed material facts will not preclude the trial court  
9 from evaluating for itself the merits of jurisdictional claims.”) (quoting *Mortensen v. First Fed.*  
10 *Sav. & Loan Ass’n*, 549 F.2d 884, 891 (9th Cir. 1977)). “However, where the jurisdictional issue  
11 and substantive issues are so intertwined that the question of jurisdiction is dependent on the  
12 resolution of factual issues going to the merits, the jurisdictional determination should await a  
13 determination of the relevant facts on either a motion going to the merits or at trial.” *Augustine v.*  
14 *United States*, 704 F.2d 1074, 1077 (9th Cir. 1983). Plaintiff bears the burden of demonstrating  
15 that the Court has subject matter jurisdiction to hear the action. *See Kokkonen v. Guardian Life*  
16 *Ins. Co.*, 511 U.S. 375, 377 (1994); *Stock W., Inc. v. Confederated Tribes*, 873 F.2d 1221, 1225  
17 (9th Cir. 1989).

18           **III. DISCUSSION**

19           Defendant first argues that Plaintiffs lack Article III standing and that this action must be  
20 dismissed under Federal Rule of Civil Procedure 12(b)(1). In the alternative, Defendant argues  
21 that this action must be dismissed under Federal Rule of Civil Procedure 12(b)(6) because the  
22 Complaint fails to state a claim that entitles Plaintiffs to relief. Because the Court dismisses on the  
23 first ground, it does not reach Defendant’s alternative theory of dismissal.

24           In a class action, “federal courts lack jurisdiction if no named plaintiff has standing.”  
25 *Frank v. Gaos*, 139 S. Ct. 1041, 1046 (2019). To establish standing, Plaintiffs “must have (1)  
26 suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant,  
27 and (3) that is likely to be redressed by a favorable judicial decision.” *Spokeo, Inc. v. Robins*, 578

1 U.S. 330, 339 (2016). Plaintiffs offer two theories of injury. First, that they lost stored data on the  
2 My Book Live device because of the factory reset. Second, they face a risk of future data misuse  
3 “if [their personal data] has made its way into the hands of cyber-criminals.” Compl. ¶ 78.

4 Defendant argues that under either theory of harm, Plaintiffs lack standing. The Court agrees.

5 *First*, Plaintiffs have not demonstrated that loss of their stored data caused them to suffer  
6 an injury in fact. An injury in fact is “an invasion of a legally protected interest’ that is ‘concrete  
7 and particularized’ and ‘actual or imminent, not conjectural or hypothetical.’” *Spokeo*, 578 U.S. at  
8 339 (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992)). Plaintiffs’ first theory of  
9 injury, that they lost stored data, fails to establish that Plaintiffs suffered a “concrete and  
10 particularized” harm. Plaintiffs fail to allege any details regarding the data loss or how they were  
11 harmed by the loss. Instead, Plaintiffs blanketly allege that the data was “deleted” from the  
12 Covered Products, that they were “unable to recover the data deleted,” and that they were “harmed  
13 both personally and economically as a result.” Compl. ¶¶ 23, 29, 35, 41. Plaintiffs fail to describe  
14 whether their data was permanently lost, and/or whether another copy of the data was stored  
15 elsewhere. Further, for any data that may have been lost, Plaintiffs fail to describe the type of data  
16 lost, or explain why it was valuable and why its loss would cause harm. Instead, Plaintiffs assume  
17 that the hack itself *per se* caused harm. This is improper. Without allegations that support  
18 Plaintiffs’ assumption of harm, Plaintiffs have not established an injury in fact. *See Warth v.*  
19 *Seldin*, 422 U.S. 490, 501 (1975) (“[T]he plaintiff . . . must allege a distinct and palpable injury *to*  
20 *himself*, even if it is an injury shared by a large class of other possible litigants.” (emphasis  
21 added)).

22 *Second*, Plaintiffs’ theory that they face a risk of future data misuse fares no better. As  
23 stated, an injury in fact is an invasion of a legally protected interest that is not “conjectural or  
24 hypothetical.” *Lujan*, 504 U.S. at 560. Plaintiffs speculate that their lost data may have “made its  
25 way into the hands of cyber-criminals.” Compl. ¶ 78. Plaintiffs fail to plead any facts to support  
26 this allegation. *See* Compl. ¶ 78 (“At present, . . . [Plaintiffs] are unaware as to *whether their*  
27 *Stored Data was merely deleted*, or if such information has made its way into the hands of cyber-

1 criminals.”). Plaintiffs’ speculative allegations of harm do not establish an injury in fact. *See*  
2 *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2212 (2021) (“The plaintiffs claimed that  
3 *TransUnion could have* divulged their misleading credit information . . . . But the plaintiffs did not  
4 demonstrate a sufficient likelihood that their individual credit information would be requested by  
5 third-party businesses and provided by *TransUnion* during the relevant time period.” (emphasis  
6 added)); *see also Giroux v. Essex Prop. Trust, Inc.*, 2017 WL 1549477, at \*2 (N.D. Cal. May 1,  
7 2017) (“The only allegations that Plaintiff makes about herself are generically that she will have to  
8 remain vigilant for the rest of her life to combat potential identity theft and tax  
9 fraud,’ . . . . Without more clarity about the specific harm that Plaintiff has personally suffered, the  
10 Court cannot adequately assess whether Plaintiff has Article III standing.”).

11 *Krottner v. Starbucks Corporation*, 628 F.3d 1139 (9th Cir. 2010) provides a good point of  
12 contrast. There, a laptop was stolen from Starbucks. *Id.* at 1140. The laptop contained the  
13 unencrypted names, addresses, and social security numbers of approximately 97,000 Starbucks  
14 employees. *Id.* After the theft, the plaintiffs spent substantial time monitoring their accounts, paid  
15 for credit monitoring services, enrolled in fraud alerts, and alleged resulting anxiety and stress. *Id.*  
16 at 1141. One named plaintiff’s bank notified him that someone had tried to open an account using  
17 his social security number. *Id.* This established a “credible threat of real and immediate harm  
18 stemming from the theft of [the] laptop.” *Id.* at 1143. However, the Ninth Circuit noted that if the  
19 plaintiffs’ allegations had been “more conjectural and hypothetical—for example, if *no laptop had*  
20 *been stolen*, and Plaintiffs had sued based on the risk that it *would be* stolen at some point in the  
21 future,” the threat of harm would be “far less credible.” *Id.* (emphases added).

22 In contrast, here, Plaintiffs do not allege that through the breach, their specific personal  
23 information was stolen or that any harm has resulted from the breach (*i.e.*, through hackers).  
24 Accordingly, Plaintiffs have not alleged an injury in fact and lack Article III standing to pursue  
25 their claims. *See Foster v. Essex Prop. Trust, Inc.*, 2015 WL 7566811, at \*3 (N.D. Cal. Nov. 25,  
26 2015) (“Since Plaintiffs have not shown, . . . that any of their information was actually stolen, their  
27 theory of future harm is implausible.”); *In re LinkedIn User Privacy Litig.*, 932 F. Supp. 2d 1089,

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

1094 (N.D. Cal. 2013).

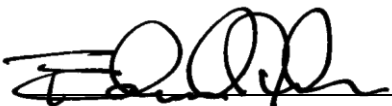
**IV. CONCLUSION**

For the foregoing reasons, the Court **GRANTS** Defendant’s motion to dismiss. When dismissing a complaint for failure to state a claim, a court should grant leave to amend “unless it determines that the pleading could not possibly be cured by the allegation of other facts.” *Lopez v. Smith*, 203 F.3d 1122, 1127 (9th Cir. 2000). Although the Court has determined that Plaintiffs have failed to plead sufficient facts to establish Article III standing, it is possible Plaintiffs can cure their allegations by alleging, among other things, more particular facts as to what data was taken and whether the data has been misused. Accordingly, the Court grants Defendant’s motion to dismiss **with leave to amend**.

Should Plaintiffs choose to file an amended complaint, they must do so by June 27, 2022. Failure to do so, or failure to cure the deficiencies addressed in this Order, will result in dismissal of Plaintiffs’ claims. Plaintiffs may not add new claims or parties without leave of the Court or stipulation by the parties pursuant to Federal Rule of Civil Procedure 15.

**IT IS SO ORDERED.**

Dated: June 7, 2022

  
EDWARD J. DAVILA  
United States District Judge