

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

JUAN FLORES-MENDEZ, an individual
and AMBER COLLINS, an individual, and
on behalf of classes of similarly situated
individuals,

No. C 20-04929 WHA

Plaintiffs,

v.

**ORDER RE MOTIONS TO AMEND
AND DISMISS**

ZOOSK, INC., a Delaware corporation,
Defendant.

INTRODUCTION

In this putative class action by data-breach victims, plaintiffs move for leave to file their second amended complaint. Defendant moves to dismiss the second claim for relief. For the reasons that follow, plaintiffs' motion to amend is **GRANTED**. The motion to dismiss is also **GRANTED**.

STATEMENT

A prior order details the facts of this action (Dkt. No. 61). In short, plaintiffs Juan Flores-Mendez and Amber Collins subscribe to defendant Zoosk, Inc.'s free dating platform. Plaintiffs had the options to join Zoosk for free or to pay for a premium subscription service. Customers provide their personal information to Zoosk upon joining. Zoosk's privacy policy, which

1 allegedly contains the company's data-security-related representations, is generally directed to
 2 its customers when they join. Plaintiffs allege injury from a massive data breach, which
 3 allegedly occurred because Zoosk failed to protect plaintiffs' personal information adequately.
 4 The proposed second amended complaint newly alleges that before the announcement of the
 5 data breach, plaintiff Flores-Mendez *paid for* a premium subscription service. It further alleges
 6 a subclass of other Zoosk subscription customers like Flores-Mendez (the subscription subclass).
 7 Collins and others did not pay for Zoosk services (Sec. Amd. Compl. ¶¶ 2, 3, 27, 32-35; Br. at
 8 6; Rep. Br. at 3-4).

9 A prior order herein dated January 30, 2021, granted in part and denied in part Zoosk's
 10 motion to dismiss the first amended complaint, noting that it had not alleged a claim for relief
 11 under California's Unfair Competition Law at California Business & Professions Code Section
 12 17200 (Dkt. No. 61).

13 Plaintiffs now file a proposed second amended complaint concurrently with their motion
 14 for leave to amend. In the proposed second amended complaint, plaintiffs attempt to cure the
 15 deficiencies in their rejected Section 17200 claim. In addition, the second amended complaint
 16 would delete former-defendant Spark Networks, SE, from this action without prejudice (Br. at
 17 78). Zoosk opposes the motion to amend as to the Section 17200 claim and moves to dismiss
 18 the Section 17200 claim.

19 This order follows full briefing and a telephonic hearing.

20 ANALYSIS

21 1. PLAINTIFFS' MOTION FOR LEAVE TO AMEND.

22 To the extent stated at the hearing, the motion to amend is **GRANTED**.

23 2. DEFENDANT'S MOTION TO DISMISS.

24 Zoosk maintains, just as it did at the first motion to dismiss, that plaintiffs lack standing to
 25 bring a Section 17200 claim because they have failed to allege that Zoosk's wrongdoing caused
 26 economic injury, a necessary precondition for entitlement to relief under Section 17200 (Br. at
 27 4). This order agrees.
 28

To qualify for relief, plaintiffs must show “a loss of money or property caused by unfair competition.” Cal. Bus. & Prof. Code § 17204. “There are innumerable ways in which economic injury from unfair competition may be shown.” *Kwikset Corp. v. Superior Ct.*, 51 Cal. 4th 310, 323 (2011). A plaintiff may, for instance,

(1) surrender in a transaction more, or acquire in a transaction less, than he or she otherwise would have; (2) have a present or future property interest diminished; (3) be deprived of money or property to which he or she has a cognizable claim; or (4) be required to enter into a transaction, costing money or property, that would otherwise have been unnecessary.

Ibid.

Our prior order found that plaintiffs’ first amended complaint had not sufficiently alleged a Section 17200 claim (Dkt. No. 61 at 7):

So far, plaintiffs have alleged a loss of privacy, heightened risk of future identity theft, loss of time, and anxiety. They do not, for example, allege that they had to buy credit-monitoring services, nor do they adequately allege the value of their time in terms of opportunity cost.

The second amended complaint has modified plaintiffs’ claims to allege harm by detailing (a) the subscription subclass, and (b) that, had plaintiffs known that their personal information would not be adequately secured and protected, they would not have used Zoosk’s services (Sec. Amd. Compl. ¶¶ 93, 97):

Additionally, Defendant collected money from the Subscription Subclass but failed to commit appropriate portions of that money to enact security measures to protect Plaintiffs’ and Class Members’ PII

Had Plaintiffs known that their PII would not be adequately secured and protected, they would not have used Defendant’s services.

The second amended complaint also alleges (Sec. Amd. Compl. ¶ 35):

Zoosk’s Privacy Policy assures Zoosk customers their PII is secure. For example, Zoosk states it “At Zoosk, we value your privacy and trust” and “work[s] with third parties to employ technologies . . . to ensure the safety and security of your data. . . .”

The latter quotation refers, in fact, to Zoosk’s policy regarding cross-platform security (Br. at 4; Sec. Amd. Compl. n. 7, emphasis added):

We also work with third parties to employ technologies, including the application of statistical modelling tools, which attempt to recognize you across multiple devices so that we understand how you use our Service across various devices, *to ensure the safety and security of your data and the Zoosk Services . . .*

This order now addresses claims of plaintiffs who did not pay for Zoosk’s premium service, *i.e.* the non-subscription class members. It will then address claims of those who did, *i.e.* the subscription subclass members.

A. SECTION 17200 STANDING FOR NON-SUBSCRIPTION CLASS MEMBERS.

For the non-subscription members, this order finds that the amended complaint once again fails to allege a “loss of money or property.” Our prior order dispensed with plaintiffs’ argument that the loss of their personal information constitutes an economic loss for Section 17200-standing purposes (Dkt. Nos. 85 at 3, 61 at 7). Notably, plaintiffs have provided market valuation for the personal information but have not specified how the data breach impaired *their* ability to participate in the market for that information. This lack of specificity is fatal. The non-subscription class members also cannot prevail on a restitution theory. Our court of appeals recently held that “the traditional principles governing equitable remedies in federal courts, including the requisite inadequacy of legal remedies, apply when a party requests restitution under the UCL and CLRA in a diversity action.” *Sonner v. Premier Nutrition Co.*, 971 F.3d 834, 844 (9th Cir. 2020). “The object of restitution is to restore the status quo by returning to the plaintiff funds in which he or she has an ownership interest.” *Korea Supply Co. v. Lockheed Martin Corp.*, 63 P.3d 937, 947 (Cal. 2003). This is a diversity action. Plaintiffs do not state or otherwise explain how they “lack an adequate remedy at law,” so inclusion of a restitution theory is unavailing. *Sonner*, 971 F.3d at 844.

B. SECTION 17200 STANDING FOR SUBSCRIPTION SUBCLASS MEMBERS.

First, for the reasons stated above, this order rejects the subscription subclass’ argument that loss of personal information constitutes an economic loss for purposes of Section 17200 standing (Sec. Amd. Compl. ¶ 97).

As for the subscription subclass members, this order finds that they have presented a close call regarding their Section 17200 standing on an “overpayment” theory, but ultimately do not allege sufficient facts for statutory standing. *Kwikset* found a complaint to have adequately alleged Section 17200 standing when:

(1) Kwikset labeled certain locksets with “Made in U.S.A.” or a similar designation, (2) these representations were false, (3) plaintiffs saw and relied on the labels for their truth in purchasing Kwikset’s locksets, and (4) plaintiffs would not have bought the locksets otherwise.

Kwikset Corp., 51 Cal. 4th 310 at 328. To be clear, a plaintiff need not allege that the representation was the but-for cause of plaintiff’s purchase, but only that it in part induced her to “surrender in a transaction more, or acquire in a transaction less, than he or she otherwise would have.” *Id.* at 323.

Our parties dispute (3) only. The argument, however, breaks down into two steps: *first*, plaintiffs must have alleged that they “saw and relied on” Zoosk’s alleged misrepresentations about its data-security practices, and, *second*, that they considered this “in purchasing” Zoosk’s service.

First, plaintiffs have not alleged enough awareness or consideration. *Kwikset* held that alleging economic loss requires “a showing of a causal connection or reliance on the alleged misrepresentation.” *Id.* at 326, citing *Hall v. Time Inc.*, 158 Cal. App. 4th 847, 855 (2008), as modified (Jan. 28, 2008). District courts have regularly upheld Section 17200 standing where plaintiffs alleged at least an awareness of a defendants’ data-security-related representation(s) *and* alleged that they would not have paid for or would have paid less for defendants’ services had they known about the representations’ falsity.

1 All district court decisions that had green-lighted the causal component of the *Kwiskset* test
2 involved complaints with stronger allegations that the plaintiffs actually considered the
3 misleading statements before purchasing. In *In re Adobe Sys., Inc. Priv. Litig.*, 66 F. Supp. 3d
4 1197 (N.D. Cal. 2014) (Judge Lucy Koh), the complaint alleged that the plaintiffs had “read and
5 relied on” Adobe’s data-security representations (and that they would have paid less, had they
6 known the statements were false). Consolidated Class Action Complaint, *In re Adobe Sys., Inc.*
7 *Priv. Litig.*, No. 13-05226-LHK (N.D. Cal. Apr. 4, 2014) ECF No. 39 ¶¶ 84, 91.

8 Not all district courts have focused on plaintiffs’ awareness of the allegedly misleading
9 statements. Nonetheless, successful complaints have alleged stronger facts than ours: In *In re*
10 *Marriott Int’l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447 (D. Md. 2020)
11 (Judge Paul W. Grimm), another data breach case in which the plaintiffs raised Section 17200
12 claims, the allegedly misleading privacy statement included language binding users to the terms
13 and conditions by dint of using the defendant’s website. *In re Marriott Int’l*, 440 F. Supp. 3d at
14 482 (cleaned up). The *Marriott* complaint differed in that Zoosk’s privacy policy was not
15 allegedly incorporated into Zoosk’s terms and conditions. In *McCoy v. Alphabet, Inc.*, No. 20-
16 CV-05427-SVK, 2021 WL 405816 (N.D. Cal. Feb. 2, 2021) (Judge Susan van Keulen), the
17 plaintiff successfully established standing when he alleged that that he had agreed to abide by
18 defendant’s Terms of Service (TOS), a document which incorporated defendant’s privacy
19 policy. Class Action Complaint & Demand for Jury Trial, *McCoy v. Alphabet, Inc.*, No. 20-
20 05427-SVK (N.D. Cal. Aug. 5, 2020) ECF No. 1 ¶¶ 138, 140, 145. Again, the *McCoy* plaintiffs
21 could be assumed to know the privacy policies, since they were bound to the TOS.

22 In an even closer call, *In re Anthem, Inc. Data Breach Litig.*, No. 15-MD-02617-LHK,
23 2016 WL 3029783 (N.D. Cal. May 27, 2016) (Judge Lucy Koh), the plaintiffs had standing
24 when the complaint alleged that the defendants’ privacy policy was “made available to Anthem
25 customers and to the public in many Anthem documents and websites,” and the defendants had
26 “advertised their services on their websites, including advertising privacy policies.” Second
27 Consolidated Amended Class Action Complaint, *In re Anthem, Inc. Data Breach Litig.*, No. 15-
28 02617-LHK (N.D. Cal. Mar. 11, 2016) ECF No. 473-3 ¶¶ 167, 178 523, 542(b) (emphasis

added). Our complaint, however, fails to allege when and how Zoosk subscribers encountered the allegedly misleading statements.

In *Ehret v. Uber Techs., Inc.*, 68 F. Supp. 3d 1121 (N.D. Cal. 2014) (Judge Edward M. Chen), plaintiffs alleged that Uber advertised “on its website and on its app” that 20% of their fee flows to the driver as a tip (the alleged falsehood). Amended Complaint, *Ehret v. Uber Techs., Inc.*, No. 14-113-EMC (N.D. Cal. Apr. 28, 2014) ECF No. 40 ¶ 12. Customers would have been expected to see the statement on the application itself (if not also on the website).

In contrast, in *Hall*, 158 Cal. App. 4th at 852, a decision that the *Kwikset* decision discussed, the plaintiff failed to establish standing because he did not allege that the defendant’s misrepresentations *caused* him to pay money for that defendant’s product (a book) or that he would otherwise have returned the book to avoid payment. As in *Hall*, our second amended complaint states simply that Zoosk “failed to commit appropriate” money to PII protection, that its policy “assures” customers of security, and “had plaintiffs known” they would not have “used” Zoosk. The second amended complaint has failed to allege that the subscriber plaintiffs *knew of* and *considered* Zoosk’s privacy misrepresentations at the time of purchase, either by reading the statement or because it appeared in any of the materials he saw (binding terms of service, advertisements, *etc.*). The facts of this action align best with *Hall*.

This order next addresses Zoosk’s argument that plaintiffs have not alleged payment “in connection with” Zoosk’s representations (Br. at 2). It does so solely because the issue may arise in a future amendment. Zoosk’s argument on this point fails.

Zoosk argues that standing cannot succeed because the privacy policy benefits its users “generally.” The promises apply to them immediately upon joining Zoosk’s free service. Members thus “cannot have overpaid any amount by reason of any non-performance of those promises and representations” in the Zoosk Privacy Policy (Rep. Br. at 4). This order disagrees. Just because a privacy policy applies to nonpaying and paying users alike does not imply that the paying users do not credit and value the privacy representations when choosing to spend their hard-earned money for the company’s additional services. Without the privacy promises, customers would have paid less or nothing at all (or so our plaintiffs allege). This provides a

reasonable inference that plaintiffs believed Zoosk would use subscribers' revenue in part for data security, especially since (as our previous order stated), "A dating app contains sensitive information about sexual preferences, which means that a hack and subsequent use of the private information could plausibly lead to blackmail and embarrassment" (Dkt. No. 61, at 6).

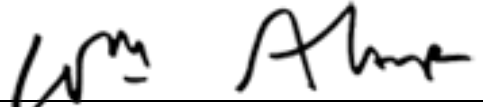
Not one of Zoosk's cited decisions required an allegation that plaintiffs believed their money would go to *additional* data security. The policy in *In re Marriott*, for instance, applied to all who logged in to Marriott's website for free, even before they booked a stay. The implication is that the *Marriott* complaint did not specifically allege that the plaintiffs believed their payment went to *more* data-security measures than Marriott had already promised in its privacy policy.

CONCLUSION

For the foregoing reasons, this order **GRANTS** Zoosk's motion to dismiss to the extent stated above. Plaintiffs are invited to move for leave to amend, with respect to the Section 17200 claim. Any motion shall be due by **OCTOBER 28 AT NOON**. Any such motion must include as an exhibit a redlined version of the proposed amendment that clearly identifies all changes from the current complaint. This order highlighted certain deficiencies in the complaint, but it will not necessarily be enough to add sentences parroting each missing item identified herein or doing what this order calls "the bare minimum." If plaintiffs move for leave to file another amended complaint, they should be sure to plead their best case and account for all criticisms, including those not reached by this order.

IT IS SO ORDERED.

Dated: October 5, 2021.


 WILLIAM ALSUP
 UNITED STATES DISTRICT JUDGE