

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

MICHAEL GREENSTEIN, et al.,
Plaintiffs,
v.
NOBLR RECIPROCAL EXCHANGE,
Defendant.

Case No. 21-cv-04537-JSW

**ORDER GRANTING MOTION TO
DISMISS SECOND AMENDED CLASS
ACTION COMPLAINT**

Re: Dkt. No. 42

Now before the Court for consideration is the motion to dismiss Plaintiffs’ second amended complaint (“SAC”) filed by Defendant Noblr Reciprocal Exchange (“Noblr” or “Defendant”). The Court has considered the parties’ papers, relevant legal authority, and the record in the case, and it finds this matter suitable for disposition without oral argument. *See* N.D. Civ. L-R 7-1(b). The Court **HEREBY GRANTS** the motion to dismiss with leave to amend.

BACKGROUND

The Court recited the factual background underlying this dispute in its Order granting Defendant’s motion to dismiss the corrected first amended class complaint. *See Greenstein v. Noblr Reciprocal Exch.*, 585 F. Supp. 3d 1220, 1224-25 (N.D. Cal. 2022). In brief, Plaintiffs and the Class Members allege that they received a letter from Noblr, dated May 14, 2021, that informed Plaintiffs that their personal information (“PI”) may have been compromised, including Plaintiffs’ driver’s license numbers, name, and address. Plaintiffs allege that they and the Class Members face an imminent threat of future harm in the form of identity theft and fraud, and that they have suffered both economic and non-economic damages, and actual injury. Plaintiffs also

1 argue that their stolen driver’s license numbers are highly sensitive PI that can result in future
2 harm. Each named Plaintiff claims that they incurred injury from increased effort and time spent
3 monitoring their credit reports.

4 The Plaintiffs and the Class Members bring the following causes of action: (1) violations
5 of the Drivers’ Privacy Protection Act (“DPPA”), 18 U.S.C. section 2724; (2) negligence; (3)
6 violation of California’s Unfair Competition Law, California Business & Professions Code section
7 17200, *et seq.* (“UCL”); and (4) declaratory and injunctive relief.

8 In dismissing the First Amended Complaint (“FAC”), the Court determined that the
9 exposed PI (names, address, and driver’s license numbers) was not sufficient to allege a credible
10 threat of future identity theft. The Court also determined that Plaintiffs have suffered no tangible,
11 monetary, or property loss. Further, the Court held that in the absence of an imminent risk of
12 harm, Plaintiffs could not rely on costs incurred in monitoring their credit to establish standing.
13 The Court also found that the Plaintiffs could not show a nexus between the alleged harm flowing
14 from the delayed notification and Noblr’s actions, and so Plaintiffs had failed to adequately allege
15 causation. Finally, the Court determined that Plaintiffs’ alleged harm would not be redressed by a
16 favorable decision.

17 The Court will address other facts as necessary in the analysis.

18 ANALYSIS

19 A. Legal Standards on the Motion to Dismiss for Lack of Subject Matter Jurisdiction.

20 The Court evaluates challenges to Article III standing under Federal Rule of Civil
21 Procedure 12(b)(1). *Maya v. Centex Corp.*, 658 F.3d 1060, 1067 (9th Cir. 2011) (motion to
22 dismiss for lack of standing governed by Rule 12(b)(1)). Where, as here, a defendant makes a
23 facial attack on jurisdiction, the factual allegations of the complaint are taken as true. *Fed’n of*
24 *African Am. Contractors v. City of Oakland*, 96 F.3d 1204, 1207 (9th Cir. 1996). Plaintiffs are
25 then entitled to have those facts construed in the light most favorable to them. *Id.*

26 The “irreducible constitutional minimum” of standing consists of three elements: an injury-
27 in-fact, causation, and redressability. *Spokeo v. Robins*, 136 S. Ct. 1540, 1547 (2016) (citing
28 *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560-61 (1992)). Plaintiffs must prove each element with

1 the same manner and degree of evidence required at each stage of the litigation. *Lujan*, 504 U.S.
2 at 561. “At the pleading stage, general factual allegations of injury resulting from the defendant’s
3 conduct may suffice, for on a motion to dismiss we ‘presum[e] that general allegations embrace
4 those specific facts that are necessary to support the claim.’” *Id.* at 561 (quoting *Lujan v. Nat’l*
5 *Wildlife Fed’n*, 497 U.S. 871, 889 (1990)). Because Plaintiffs are the parties invoking federal
6 jurisdiction, they “bear[] the burden of establishing these elements.” *Id.*

7 In a class action, standing exists where at least one named plaintiff meets these
8 requirements. *Ollier v. Sweetwater Union High Sch. Dist.*, 768 F.3d 843, 865 (9th Cir. 2014). To
9 demonstrate standing, the “named plaintiffs who represent a class must allege and show they
10 personally have been injured, not that injury has been suffered by other, unidentified members of
11 the class to which they belong and which they purport to represent.” *Lewis v. Casey*, 518 U.S.
12 343, 347 (1996) (internal quotation marks omitted). At least one named plaintiff must have
13 standing with respect to each claim that the class representatives seek to bring. *In re Ditropan XL*
14 *Antitrust Litig.*, 529 F. Supp. 2d 1098, 1107 (N.D. Cal. 2007).

15 In the context of requests for injunctive relief, the standing inquiry requires plaintiffs to
16 “demonstrate that [they have] suffered or [are] threatened with a ‘concrete and particularized’
17 legal harm, coupled with a ‘sufficient likelihood that [they] will again be wronged in a similar
18 way.’” *Bates v. United Parcel Service, Inc.*, 511 F.3d 974, 985 (9th Cir. 2007) (quoting *Lujan*,
19 504 U.S. at 560, and *City of Los Angeles v. Lyons*, 461 U.S. 95, 111 (1983)). The latter inquiry
20 turns on whether the plaintiff has a “real and immediate threat of repeated injury.” *Id.* The threat
21 of future injury cannot be “conjectural or hypothetical” but must be “certainly impending” to
22 constitute an injury in fact for injunctive relief purposes. *In re Zappos.com, Inc. (Zappos)*, 888
23 F.3d 1020, 1026 (9th Cir. 2018).

24 **B. Plaintiffs’ Fail to Correct the Deficiencies from their First Amended Complaint.**

25 According to Noblr, Plaintiffs have not alleged any new facts that would alter the Court’s
26 findings regarding the earlier iteration of the complaint. Plaintiffs argue that their amended
27 complaint makes clear that theft of driver’s license information is sufficient to post imminent risk
28 of harm. As will be discussed below, the Court agrees with Noblr.

1 **1. There Continues to be No Cognizable Threat of Future Harm.**

2 **a. The type of PI does not pose an imminent risk of harm.**

3 Instead of providing any new facts regarding the type of data that was exposed, Plaintiffs’
 4 most recent complaint provides only new arguments as to why driver’s license data should be
 5 considered sensitive PI for standing purposes. While the Court acknowledges that it is a close
 6 call, the Court continues to hold that driver’s license numbers are not as sensitive as social security
 7 numbers, and that they do not rise to the level of sensitive PI needed to establish a credible and
 8 imminent threat of future harm. The Court continues to believe that it would have to hypothesize
 9 various possibilities of future harm in order to find that Plaintiffs face a risk of imminent identity
 10 theft based on the limited amount of PI. *See In re Adobe Systems Inc. Privacy Litig.*, 66 F. Supp.
 11 3d 1197, 1214-15 (N.D. Cal. 2014) (holding that plaintiffs had demonstrated an immediate harm
 12 and the risk of injury “immediate and very real” after “hackers deliberately targeted Adobe’s
 13 servers and spent several weeks collecting names, usernames, passwords, email addresses, phone
 14 numbers, mailing addresses, credit card numbers and expiration dates”); *cf Stallone v. Farmers*
 15 *Group, Inc.*, 2022 WL 10091489, at *5 (D. Nev. Oct. 15, 2022) (holding that driver’s license data,
 16 like social security numbers, derives its value in large part from its immutability). Accordingly,
 17 because the exposed PI was limited only to Plaintiffs’ names, addresses, and driver’s license
 18 numbers, the Court finds that Plaintiffs have not sufficiently alleged the credible threat of future
 19 identity theft needed to plead injury in fact.

20 **b. Plaintiffs’ PI has not lost value.**

21 Similar to the type of PI argument, Plaintiffs do not allege any new facts to address the
 22 Court’s prior holding. Because there continues to be no real and imminent threat of identity theft,
 23 Plaintiffs’ alleged mitigation measures continue not to confer standing. Further, Plaintiff Au’s
 24 claim that she suffered actual injury because her information was used to fraudulently apply for
 25 unemployment benefits continues to be insufficient. The Court still holds that the attempted
 26 fraudulent application demonstrates that the limited PI disclosed in the breach is insufficient even
 27 for unemployment benefits, much less banking or credit card accounts. Further, Plaintiffs have
 28 not provided any new facts to “establish both the existence of a market for her personal

1 information and an impairment of her ability to participate in that market.” *Svenson v. Google Inc.*
 2 (*Svenson*), No. 13-CV-04080-BLF, 2016 WL 8943301, at *9 (N.D. Cal. Dec. 21, 2016) (citing *In*
 3 *re Google, Inc. Privacy Pol’y Litig.*, No. 5:12-CV-001382-PSG, 2015 WL 4317479, at *4 (N.D.
 4 Cal. July 15, 2015)). Therefore, Plaintiffs’ allegations of diminished value of personal
 5 information continue to be insufficient to establish injury for Article III purposes. *See Agans v.*
 6 *Uber Technologies*, 2019 WL 6522843, at *3-4 (C.D. Cal. Aug. 19, 2019) (holding that a bare
 7 “contention that [a plaintiff] suffered a loss of value of [his] private information, without any more
 8 details is too abstract and speculative to support [A]rticle III standing.”) (internal citations
 9 omitted).

10 **c. Plaintiffs’ mitigation costs are insufficient to establish standing.**

11 Plaintiffs repeat their allegations that the time and effort they have spent monitoring their
 12 credit reports constitutes a cognizable injury in fact. While courts have found that credit
 13 monitoring may be “compensable where evidence shows that the need for future monitoring is a
 14 reasonably certain consequence of the defendant’s breach of duty . . . the monitoring must be
 15 ‘reasonable and necessary.’” *Corona v. Sony Pictures Entm’t, Inc.*, No. 14-cv-09600 RGK EX,
 16 2015 WL 3916744, at *4 (C.D. Cal. June 15, 2015) (citing *Potter v. Firestone Tire & Rubber Co.*,
 17 6 Cal.4th 965, 1006-07 (1993)). In *Antman II*, the court determined that “the mitigation expenses
 18 do not qualify as injury; the risk of identity theft must be real before mitigation can establish
 19 injury in fact.” *Antman v. Uber Technologies, Inc.* (“*Antman IP*”), 2018 WL 2151231, at *22–23
 20 (N.D. Cal. May 10, 2018); *see also Webb v. Injured Workers Pharm., LLC*, 2022 LEXIS 189196,
 21 at *4 (D. Mass. Oct. 17, 2022) (holding that Plaintiffs cannot manufacture harm by alleging only
 22 that they spent considerable time and effort monitoring their accounts).

23 The Ninth Circuit recognizes that “mitigation expenses do not qualify as injury; the risk of
 24 identity theft must first be real and imminent, and not speculative, before mitigation costs establish
 25 injury in fact.” *Krottner v. Starbucks, Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010). In addition,
 26 Plaintiffs must show that the mitigation costs were reasonable and necessary. *See Holly v. Alta*
 27 *Newport Hosp., Inc.*, 2020 WL 1853308, at *6 (C.D. Cal. Apr. 10, 2020) (conclusory allegations
 28 concerning mitigation were not sufficient where plaintiff did not present any supporting facts or

1 allege how any credit monitoring was reasonable and necessary). In *In re Adobe*, the court found
 2 the financial costs incurred on data monitoring services to mitigate the data breach’s harm was a
 3 cognizable injury. 66 F. Supp. 3d at 1217. However, the court noted that “in order for costs
 4 incurred in an effort to mitigate the risk of future harm to constitute injury-in-fact, the future harm
 5 being mitigated must itself be imminent.” *Id.*

6 Plaintiffs’ effort and costs attempting to mitigate harm from the breach do not confer them
 7 standing. The Court does not consider the risk of identity theft and fraud to be real and imminent
 8 based on the type of data obtained in the Unauthorized Data Disclosure. Plaintiffs’ claims of harm
 9 are speculative in predicting that the PI will lead to identity theft without more sensitive
 10 information such as social security or routing numbers. Although Plaintiff Au once again claims
 11 that the fraudulent unemployment application demonstrates that the PI can be used for identity
 12 theft and fraud, she does not allege that the application, identity theft, or fraud was successful and
 13 resulted in her suffering any injury. In fact, the attempted fraudulent application demonstrates that
 14 the limited PI disclosed in the breach is insufficient even for unemployment benefits, much less
 15 banking or credit card accounts. Therefore, Plaintiffs’ mitigation expenses cannot establish an
 16 injury in the absence of a real and imminent risk of harm.

17 Plaintiffs Greenstein, Nelson, and Au also allege that they spent time researching and
 18 monitoring their credit information. (SAC ¶¶ 80, 86, 94.) However, Plaintiffs do not allege that
 19 their credit was harmed despite their close monitoring. Furthermore, Plaintiffs offer no factual
 20 allegations in support of the alleged credit monitoring services, nor do they sufficiently allege that
 21 such services were reasonable and necessary. Although Plaintiff Au has alleged out of pocket
 22 expenses allegedly spent on credit monitoring services, she has not provided any reason regarding
 23 why this subscription service was reasonable and necessary. Thus, in the absence of an imminent
 24 risk of harm, Plaintiffs cannot manufacture standing through costs incurred in monitoring their
 25 credit.

26 **2. No Real Injury Can Be Traced to Noblr’s Conduct.**

27 Plaintiffs continue to argue that Noblr’s actions and conduct caused them a substantial risk
 28 of harm. Plaintiffs must “[show] that the defendant’s actual action has caused the substantial risk

1 of harm.” *Clapper v. Amnesty International USA*, 568 U.S. 398, 414 (2013). In *Clapper*, the
2 Supreme Court found there was no substantial risk because plaintiffs’ theory of injury and causal
3 connection was too inferential and speculative to “satisfy the ‘fairly traceable’ requirement. *Id.* at
4 413.

5 By contrast, the plaintiffs in *Krottner* did not rely on speculation or inferences to
6 demonstrate a clear causal connection. The thief in *Krottner* stole a laptop that contained all the
7 information required for the identity theft plaintiffs suffered. 628 F.3d at 1142. Article III
8 requires “a causal connection between the injury and the conduct complained of—the injury has to
9 be ‘fairly . . . trace[able] to the challenged action of the defendant, and not . . . th[e] result [of] the
10 independent action of some third party not before the court.’” *Lujan*, 504 U.S. at 560-61 (quoting
11 *Simon v. E. Ky. Welfare Rights Org.*, 426 U.S. 26, 41-42 (1976) (ellipses in original)).

12 Plaintiffs still cannot establish that Noblr’s conduct caused them an injury in fact. Now or
13 in the future, it would be difficult to trace any future identity theft or fraud to Noblr’s specific
14 Unauthorized Data Disclosure. Plaintiffs in fact concede that “[i]n most cases, stolen data is rarely
15 attributed to the source when it is sold,” and that “stolen data is often obfuscated, parsed, and sold
16 in pieces [and] also often combined with other stolen data, further making attribution to the source
17 very difficult. (SAC ¶ 96.) Information is widely available on the internet and later data breaches
18 could reveal more personal information. Moreover, Plaintiffs do not acknowledge that it would be
19 difficult to commit fraud or identity theft with names, addresses, and driver’s license numbers
20 alone. *See Antman II*, 2018 WL 2151232, at *22 (concluding that “[w]ithout a hack of
21 information such as social security numbers, account numbers, or credit card numbers, there is no
22 obvious, credible risk of identity theft that risks real, immediate injury”). Therefore, any
23 supplemental, highly sensitive information used to commit future acts of identity theft or fraud
24 could not be specifically traced back to the data exposed by the Unauthorized Data Disclosure.

25 Furthermore, although Plaintiff Au argues close temporal proximity, she cannot trace the
26 data used for the fraudulent application to the Unauthorized Data Disclosure. Additionally,
27 Plaintiff Au fails to allege a specific connection between the breach and the type of data used in
28 the application. Even if the Unauthorized Data Disclosure occurred shortly before, Plaintiff Au

1 still has not sufficiently showed that the fraudulent application was a result of the Unauthorized
2 Data Disclosure itself. In fact, since Noblr’s instant quote feature used information that was
3 already available online, it is possible that the data used for the fraudulent application could have
4 been obtained from a third-party or unrelated data breach.

5 Plaintiffs further allege that Noblr’s delay in identifying and reporting the breach caused
6 them additional harm. (SAC ¶ 51.) Delay of notification is insufficient to establish injury-in-fact.
7 *In re Adobe*, 66 F. Supp. 3d at 1218. In *In re Adobe*, the court determined that that Plaintiff had
8 failed to allege injury in fact because Plaintiff had not traced any injury from the delayed
9 notification. *Id.* at 1217. Moreover, the court in *Antman II* determined that “delay alone is not
10 enough.” *Antman II*, 2018 WL 2151232, at *23 (citing *Remijas v. Neiman Marcus Grp., LLC*, 794
11 F.3d 688, 695 (7th Cir. 2015) (“delay in notification,” on its own, “is not a cognizable injury” that
12 confers Article III standing on a plaintiff) (citing *Price v. Starbucks Corp.*, 192 Cal. App. 4th
13 1136, 1143 (2011)); *In re Adobe*, 66 F. Supp. 3d at 1217-18 (concluding that the plaintiffs had not
14 established Article III standing based on the defendant’s alleged failure to reasonably notify them
15 of the data breach because the plaintiffs did “not allege that they suffered any incremental harm as
16 a result of the delay”).

17 Similar to the plaintiffs in *In re Adobe*, Plaintiffs have not alleged any specific injury
18 traceable to Noblr because Plaintiffs do not allege that they suffered any incremental harm because
19 of the delay. 66 F. Supp. 3d at 1217. Plaintiffs have supplemented their complaint to add that the
20 four-month delay prevented the police from detection or the Plaintiffs from beginning remedial
21 action. (SAC ¶ 51.) However, the Court finds that Plaintiffs still have not traced any specific
22 harm from Noblr’s delayed notification and cannot show a nexus between the alleged harm
23 flowing from the delayed notification and Noblr’s actions. Accordingly, Plaintiffs have failed to
24 adequately alleged causation.

25 3. Plaintiffs’ Alleged Harm Will Not be Redressed By a Favorable Decision.

26 Plaintiffs argue that a favorable judicial decision will redress the harm caused by the
27 Unauthorized Data Disclosure. “[I]t must be ‘likely,’ as opposed to merely ‘speculative,’ that the
28 injury will be redressed by a favorable decision.” *Lujan*, 504 U.S. at 560-61 (internal quotations

1 and citations omitted). Plaintiffs allege: (1) Noblr used unsafe and insecure methods of
2 safeguarding Plaintiffs' PI, (SAC ¶¶ 55-56, 64); (2) Noblr had access to Plaintiffs' PI, (*Id.* ¶¶ 18-
3 22); (3) attackers could target Plaintiffs' PI, including their driver's licenses numbers and
4 addresses, (*Id.* ¶¶ 21-27); and (4) attackers' access to driver's license information creates a strong
5 risk of identity theft and fraud (*Id.* ¶ 27). Finally, Plaintiffs contend that Plaintiff Au's fraudulent
6 unemployment benefits application supports the strong risk of identity theft and fraud.

7 As discussed above, Plaintiff Au cannot demonstrate that the data disclosed in the
8 Unauthorized Data Disclosure was the basis for the fraudulent application. In addition, Plaintiff
9 Au does not allege she experienced any cognizable injury because of that application or any
10 employment benefits that may have been fraudulently obtained. The addition of facts regarding
11 the darkweb and the diminution of the value of her PI does not change the Court's previous
12 analysis.

13 Plaintiffs next argue that the Unauthorized Data Disclosure resulted in a strong risk or high
14 likelihood of identity theft and fraud. Besides failing to demonstrate a strong risk of future
15 identity theft, Plaintiffs also fail to explain how unknown future harm will occur. For instance,
16 Plaintiffs do not explain how names, addresses, and driver's license numbers, without more
17 sensitive information, can be used successfully to commit identity theft. It remains inappropriate
18 for this Court to not only speculate about future harm, but whether a future decision would redress
19 hypothetical harm.

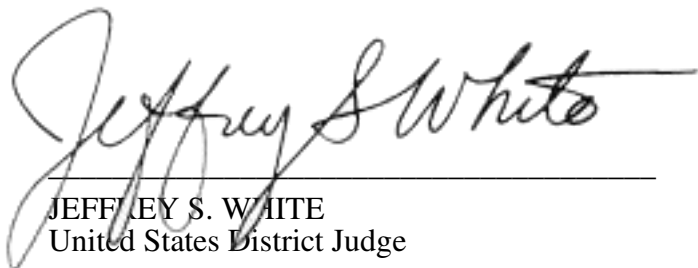
20 Although Plaintiffs request injunctive relief, that relief would have little impact on the PI
21 that was disclosed by the Unauthorized Data Disclosure. Injunctive or declaratory relief would
22 not be able to redress any future harm of identity theft or fraud because it could not compel the
23 hackers or Noblr to return the PI to Plaintiffs. Additionally, declaratory relief would not motivate
24 Noblr to change its practices. Noblr already took immediate action to remedy its unintentional
25 disclosure by changing its policies and masking driver's license numbers in the page source code.
26 (SAC ¶ 25.)

CONCLUSION

For the foregoing reasons, Defendant’s motion to dismiss is GRANTED. Because the Court has previously given Plaintiffs leave to amend, the Court finds dismissal with prejudice is appropriate. *See Allen v. City of Beverly Hills*, 911 F.2d 367, 373 (9th Cir. 1990). The Court shall issue a separate judgment and the Clerk is instructed to close the file.

IT IS SO ORDERED.

Dated: December 5, 2022



JEFFREY S. WHITE
United States District Judge

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