UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

San Francisco Division

SASHA ANTMAN and GUSTAVE LINK, individually and on behalf of others similarly situated,

Plaintiffs,

v.

UBER TECHNOLOGIES, INC. and Does 1–50,

Defendants.

Case No. 15-cv-01175-LB

ORDER GRANTING MOTION TO DISMISS WITH LEAVE TO AMEND

Re: ECF No. 166

INTRODUCTION

The plaintiffs are former Uber drivers who filed this class-action lawsuit against the defendant Uber Technologies — which operates a smart-phone application connecting drivers and passengers — after an unknown hacker downloaded drivers' personally identifiable information ("PII") from Uber's computer system in May 2014, an event that Uber disclosed in February 2015.[1] In October 2015, the court dismissed the First Amended Complaint ("FAC") — brought

[1] Second Amended Complaint ("SAC") – ECF No. 163 at 3 (¶¶ 11–12). Citations refer to material in the Electronic Case File ("ECF"); pinpoint citations are to the ECF-generated page numbers at the top of documents.

only by Mr. Antman — for lack of standing.[2] In part the court's analysis turned on Mr. Antman's failure to allege injury in fact because his complaint alleged only the theft of names and driver's license numbers and — without more PII disclosed, such as Social Security or account numbers — there was no plausible, immediate risk of identity theft.[3]

The parties then engaged in informal discovery and tried (unsuccessfully) to mediate the dispute.[4] The plaintiffs filed their Second Amended Complaint ("SAC"), adding Mr. Link as a named plaintiff and raising the following claims: (1) failure to implement and maintain reasonable security procedures to protect the drivers' personal information and promptly notify affected drivers, in violation of Cal. Civ. Code §§ 1798.81, 1798.81.5, and 1798.82; (2) unfair, fraudulent, and unlawful business practices, in violation of California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200; (3) negligence; and (4) breach of implied contract.[5] The first two claims are on behalf of a California class, and the third and fourth claims are on behalf of a national class or (in the alternative) a California class.[6]

Uber moves to dismiss for lack of standing under Federal Rule of Civil Procedure 12(b)(1) and for failure to plead plausible claims under Rule 12(b)(6).[7] The court grants the motion and dismisses the complaint without prejudice because the named plaintiffs lack Article III standing.

STATEMENT[8]

The named plaintiffs are Sasha Antman and Gustave Link. Both worked as Uber drivers in California.[9] They sue for Uber's failure to protect their PII "including names, driver's license

---

[2] Order – ECF No. 44 at 13–18.

[3] *Id.* at 16.

[4] Status Report – ECF No. 154.

[5] SAC – ECF No. 163 at 14–22. The previous complaint raised only the first two claims. *See* First Amended Complaint ("FAC") – ECF No. 7.

[6] SAC – ECF No. 163 at 14–22.

[7] Motion – ECF No. 166 at 9–11.

[8] Unless otherwise noted, the fact allegations in the Statement are from the SAC.

[9] SAC – ECF No. 163 at 2 (¶¶ 1–2), 6 (¶¶ 25–26).

numbers, banking information, Social Security Numbers, and other personal identifying information (collectively, 'Private Information') . . . and for failing to provide timely and adequate notice to Plaintiffs and other Class members that their Private Information had been stolen and precisely what types of information were stolen."[10]

1. The Data Breach

"Beginning in or around May 2014, an unknown person or persons (the 'Hacker') utilized what [Uber] has described as a 'security key' to download files from [its] computer system containing its drivers' Private Information (the 'Data Breach')."[11] "[T]he 'security key' used by the Hacker to perpetrate the Data Breach was publicly available on the internet via one or more GitHub webpages (and/or via the GitHub app, which is an app designed for sharing code among app developers)."[12] "In other words, [Uber] not only permitted all of the compromised Private Information to be accessible via single password, but allowed that password to be publicly accessible via the internet."[13] The plaintiffs allege on information and belief that "the Plaintiffs' and Class Members' Private Information and the password allowing access to that Private Information were improperly handled and stored, were unencrypted, and were not kept in accordance with applicable, required, and appropriate cyber-security protocols, policies, and procedures."[14]

Uber did not disclose the Data Breach until February 27, 2015.[15] On that date, Uber "disseminated a press release," which reads in its entirety as follows:

> In late 2014, we identified a one-time access of an Uber database by an unauthorized third party. A small percentage of current and former Uber driver partner names and driver's license numbers were contained in the database. Immediately upon discovery we changed the access protocols for the database, removing the possibility of

---

[10] *Id.* at 2 (¶ 8).

[11] *Id.* at 3 (¶ 11).

[12] *Id.* at 4 (¶ 17).

[13] *Id.*

[14] *Id.* at 5 (¶ 19).

[15] *Id.* at 2 (¶ 12).

unauthorized access. We are notifying impacted drivers, but we have not received any reports of actual misuse of information as a result of this incident.

Uber takes seriously our responsibility to safeguard personal information, and we are sorry for any inconvenience this incident may cause. In addition, today we filed a lawsuit that will enable us to gather information to help identify and prosecute this unauthorized third party.

Here is what we know:

- On September 17, 2014, we discovered that one of our databases could potentially have been accessed by a third party.
- Upon discovery we immediately changed the access protocols for the database and began an in-depth investigation.
- Our investigation revealed that a one-time unauthorized access to an Uber database by a third party had occurred on May 13, 2014.
- Our investigation determined the unauthorized access impacted approximately 50,000 drivers across multiple states, which is a small percentage of current and former Uber driver partners.
- The files that were accessed contained only the name and driver's license number of some driver partners.
- To date, we have not received any reports of actual misuse of any information as a result of this incident, but we are notifying impacted drivers and recommend these individuals monitor their credit reports for fraudulent transactions or accounts.
- Uber will provide a free one-year membership of Experian's® ProtectMyID® Alert. If impacted driver partners have questions or need an alternative to enrolling online, please call (877) 297-7780 and provide the Engagement number listed in the notification letter.
- We have also filed what is referred to as a "John Doe" lawsuit so that we are able to gather information that may lead to confirmation of the identity of the third party.[16]

In August 2016 (after the court's October 2015 order dismissing the FAC), Uber issued a second notice to some "victims of the Data Breach informing them that additional Private Information was disclosed in the Data Breach . . . and offering another year of credit monitoring."[17] The SAC specifies that the additional private information "include[d] banking

[16] Wong Decl. – ECF No. 24-1 at 4–5; *see also* SAC – ECF No. 163 at 3–4 (¶ 12) (citing the link to the online press release), ¶¶ 13–17 (citing press release)). The court considers the entire press release under the incorporation-by-reference doctrine. *See Knievel v. ESPN*, 393 F.3d 1068, 1076 (9th Cir. 2005).

[17] SAC – ECF No. 163 at 5 (¶ 21).

information and Social Security Numbers, in addition to driver's license numbers and names."[18]

2. Harm to the Named Plaintiffs

Mr. Antman worked as an Uber driver in San Francisco, California, "receiving his last payment for such services in or around September 2013."[19] "On or around June 2, 2014, an unknown and unauthorized person used [his] Private Information to apply for a credit card with Capital One, which now appears on [his] credit report."[20] Mr. Antman "received a First Breach Notification from [Uber] in or around March 2015, notifying him for the first time that his Private Information was disclosed in the Data Breach, even though he no longer was working as an Uber driver at the time of the Data Breach."[21] (The first notice disclosed to affected drivers that their names and driver's license numbers were compromised in the hack.) He "also received a Second Breach Notification in or around August 26, 2016, via email, notifying him that, in fact, more of his Private Information was disclosed in the Data Breach than was referenced in the First Breach Notification, including his banking information."[22]

Mr. Link worked as an Uber driver in the San Francisco Bay Area from approximately August 2012 until January 2015.[23]

> Plaintiffs' investigation has revealed, and on that basis they are informed and believe, that following the Data Breach both Plaintiffs' Private Information, including their Social Security Numbers, have been made available for sale on the "dark web." Neither Plaintiff has received notification that similar information has been disclosed as a result of some other data breach.[24]

The plaintiffs submitted a declaration with additional facts about Mr. Link and ask for leave to amend the complaint to include them.[25] He received the first notice in February 2015 that his name

---

[18] *Id.* (¶ 22).

[19] *Id.* at 6 (¶ 25)

[20] *Id.* (¶ 27).

[21] *Id.* (¶ 28).

[22] *Id.* at 6–7 (¶ 29).

[23] *Id.* at 6 (¶ 26).

[24] *Id.* at 7 (¶ 30).

[25] Opposition to Motion to Dismiss – ECF No. 168 at 6–7; Link Decl. – ECF No. 168-1 at 2–3.

and driver's license number were disclosed in the data breach.[26] On August 20, 2015, the IRS rejected his tax filing for the December 31, 2014 tax period.[27] He later learned that someone used his Social Security number to file fraudulent tax returns in his name. He spent hours addressing the incident and refiling his return. His refund was delayed over eight months, and he has spent and continues to spend significant time to ensure that his credit and identity have not been compromised further.[28]

Uber's notifications to Mr. Antman and Mr. Link did not "include[] any explanation for the long delay in their issuance, or indicate that the delay was due to any law enforcement investigation."[29] "Plaintiff Antman spent significant time addressing the Data Breach (*see, e.g.*, ECF No. 30-1, Declaration of Sasha Antman), and Plaintiff Link has incurred costs and spent time monitoring his credit."[30]

3. Harm to Class Members

"Plaintiffs and other Class Members suffered injuries including but not limited to time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, invasion of their privacy, and loss of value of their Private Information."[31] The next section of the complaint is titled "The Stolen Private Information Is Valuable to Hackers and Thieves and Its Disclosure Harms Class Members."[32] It includes the following points:

- The Private Information is valuable and "as good as gold to identity thieves."
- Social Security numbers are particularly valuable; criminals use them to create false bank accounts, file fraudulent bank returns, and incur credit in the victim's name.
- There may be a lag time (in some cases, up to a year or more) between when Private

[26] Link Decl. – ECF No. 168-1 at 2 (¶ 5), 5.
[27] *Id.* at 2 (¶¶ 6–7), 7–8.
[28] *Id.* at 2–3 (¶¶ 7–11).
[29] SAC – ECF No. 163 at 7 (¶ 31).
[30] *Id.* (¶ 32).
[31] *Id.* (¶ 33).
[32] *Id.* at 7.

Information is stolen and when it is used. Once stolen data is posted on the Internet, fraudulent use may continue for years.

- "The plaintiffs and class members face years of years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges incurred by them and the resulting loss of use of their credit and access to funds, whether or not such charges are ultimately reimbursed by the credit card companies."[33]

4. Relief Sought

The complaint alleges the following class claims: (1) failure to implement and maintain reasonable security procedures to protect the drivers' personal information and promptly notify affected drivers, in violation of Cal. Civ. Code §§ 1798.81, 1798.81.5, and 1798.82; (2) unfair, fraudulent, and unlawful business practices, in violation of California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200; (3) negligence; and (4) breach of implied contract.[34]

The first two claims are on behalf of a California class, defined as "All persons residing in California whose personal information was disclosed in the data breach affecting Uber Technologies, Inc. in 2014."[35] The third and fourth claims are on behalf of a national class or (in the alternative) a California class. The national class is defined as "All persons residing in the United States whose personal information was disclosed in the data breach affecting Uber Technologies, Inc. in 2014."[36] The plaintiffs seek injunctive relief, damages, and attorney's fees in claim one, injunctive relief and equitable relief (in the form of restitution) in claim two, and

---

[33] *Id.* at 7–11 (¶¶ 34–47).

[34] For an analysis of the requirements of Cal. Civ. Code §§ 1798.81, 1798.81.5, and 1798.82, see the court's earlier order. Order – ECF No. 44 at 7–8. The statutory scheme generally protects the "personal information" of California residents by requiring businesses that maintain personal information to take reasonable measures to protect it, has notice procedures to customers if their encrypted personal information is disclosed in a data breach, and provides a private right of action for customers injured by a violation of the statute. *Id.* The statute defines "personal information" as an individual's first name (or first initial) and last name with one or more of the following unencrypted or unredacted elements: (1) Social Security number; (2) driver's license number or California identification-card number; (3) account number or debit-card or credit-card number in combination with the security code, access code, or password that permits access to that financial account, and (4) medical information in the form of medical history, treatment, or diagnosis. Cal. Civ. Code § 1798.81.5(d).

[35] SAC – ECF No. 163 at 11–12 (¶ 50).

[36] *Id.* at 11 (¶ 49).

damages in claims three and four.[37]

GOVERNING LAW

The defendants move to dismiss the complaint under Federal Rule of Civil Procedure 12(b)(1) for lack of standing and under Federal Rule of Civil Procedure 12(b)(6) for failure to state a claim.

1. Rule 12(b)(1) Standard

A complaint must contain a short and plain statement of the ground for the court's jurisdiction. Fed. R. Civ. P. 8(a)(1). The plaintiff has the burden of establishing jurisdiction. *See Kokkonen v. Guardian Life Ins. Co. of Am.*, 511 U.S. 375, 377 (1994); *Farmers Ins. Exch. v. Portage La Prairie Mut. Ins. Co.*, 907 F.2d 911, 912 (9th Cir. 1990).

A defendant's Rule 12(b)(1) jurisdictional attack can be either facial or factual. *White v. Lee*, 227 F.3d 1214, 1242 (9th Cir. 2000). "A 'facial' attack asserts that a complaint's allegations are themselves insufficient to invoke jurisdiction, while a 'factual' attack asserts that the complaint's allegations, though adequate on their face to invoke jurisdiction, are untrue." *Courthouse News Serv. v. Planet*, 750 F.3d 776, 780 n.3 (9th Cir. 2014). This is a facial attack. The court thus "accept[s] all allegations of fact in the complaint as true and construe[s] them in the light most favorable to the plaintiffs." *Warren v. Fox Family Worldwide, Inc.*, 328 F.3d 1136, 1139 (9th Cir. 2003).

Standing pertains to the court's subject-matter jurisdiction and thus is properly raised in a Rule 12(b)(1) motion to dismiss. *See Chandler v. State Farm Mut. Auto. Ins. Co.*, 598 F.3d 1115, 1121–22 (9th Cir. 2010).

2. Rule 12(b)(6) Standard

A complaint must contain a "short and plain statement of the claim showing that the pleader is entitled to relief" to give the defendant "fair notice" of what the claims are and the grounds upon

[37] *Id.* at 15–16 (¶¶ 71–74), 18–19 (¶¶ 85–86), 21(¶¶ 97, 103).

which they rest. *See* Fed. R. Civ. P. 8(a)(2); *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). A complaint does not need detailed factual allegations, but "a plaintiff's obligation to provide the 'grounds' of his 'entitlement to relief' requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do. Factual allegations must be enough to raise a claim for relief above the speculative level . . . ." *Id.* (internal citations omitted).

To survive a motion to dismiss, a complaint must contain sufficient factual allegations, accepted as true, "'to state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Twombly*, 550 U.S. at 570). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* "The plausibility standard is not akin to a 'probability requirement,' but it asks for more than a sheer possibility that a defendant has acted unlawfully." *Id.* (quoting *Twombly*, 550 U.S. at 557). "Where a complaint pleads facts that are 'merely consistent with' a defendant's liability, it 'stops short of the line between possibility and plausibility of "entitlement to relief."'" *Id.* (quoting *Twombly*, 550 U.S. at 557).

If a court dismisses a complaint, it should give leave to amend unless the "the pleading could not possibly be cured by the allegation of other facts." *Cook, Perkiss & Liehe, Inc. v. N. Cal. Collection Serv. Inc.*, 911 F.2d 242, 247 (9th Cir. 1990).

ANALYSIS

Federal-court jurisdiction extends only to "cases" and "controversies." *Raines v. Byrd*, 521 U.S. 811, 818 (1997). "Standing to sue is a doctrine rooted in the traditional understanding of a case or controversy." *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016). To establish standing, "[t]he plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Id.* (citing *Lujan v Defenders of Wildlife*, 504 U.S. 555, 560 (1992)).

In a class action, the named plaintiffs representing a class "must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong and which they purport to represent." *Warth v. Seldin*, 422 U.S.

490, 502 (1975). "[I]f none of the named plaintiffs purporting to represent a class establishes the requisite of a case or controversy with the defendants, none may seek relief on behalf of himself or any other member of the class." *O'Shea v. Littleton*, 414 U.S. 488, 494 (1974).

Uber contends that the named plaintiffs lack Article III standing, largely for the reasons that the court advanced in its earlier order.[38] In that order, the court analyzed standing and data-breach cases and concluded that disclosure of driver's license numbers and driver names did not establish an increased risk of injury. Order – ECF No. 44 at 14–15 (applying *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1140–43 (9th Cir. 2010)). The court summarized the holding in *Krottner*:

> The controlling case in the Ninth Circuit is *Krottner v. Starbucks Corporation. See* 628 F.3d 1139 (9th Cir. 2010). The plaintiffs there were current or former Starbucks employees whose names, addresses, and social security numbers were on a laptop stolen from Starbucks. *See id.* at 1140. The named plaintiffs enrolled in the free credit-watch service that Starbucks offered them. *Id.* at 1141. Two named plaintiffs spent substantial time monitoring their accounts; one said that she would pay her out-of-pocket expenses for ongoing credit monitoring once the free service expired; another placed fraud alerts and experienced anxiety and stress. *Id.* Another named plaintiff's bank notified him that someone tried to open a new account using his social security number; the bank closed the account and the plaintiff did not allege any financial loss. *Id.* The Ninth Circuit affirmed the district court, finding injury in fact sufficient to convey Article III standing. *Id.* at 1142–43. The anxiety and stress was injury that conferred standing for one plaintiff. *Id.* at 1142. The increased risk of future identity theft was injury that conferred standing for all plaintiffs, even though their data had been stolen and not yet misused. *Id.* at 1142–43. In the identity-theft context, the court held, this was a "credible threat of real and immediate harm stemming from a theft of a laptop containing their unencrypted personal data." *Id.* at 1143. By contrast, if the plaintiffs' allegations were "more conjectural or hypothetical—for example, if no laptop had been stolen, and Plaintiffs sued based on the risk that it would be stolen at some point in the future—we would find the threat far less credible." *Id.*

Id. at 14–15. The court held that a credible threat of immediate identity theft based on stolen data is sufficient to establish injury in fact. *Id.* at 15–16 (distinguishing *Clapper v. Amnesty Int'l U.S.A.*, 568 U.S. 398, 410–14 (2015)). The court concluded:

> With that standard in mind, the court holds that Mr. Antman's allegations are not sufficient because his complaint alleges only the theft of names and driver's licenses. Without a hack of information such as social security numbers, account numbers, or credit card numbers, there is no obvious, credible risk of identity theft that risks real, immediate injury. It was that risk (in the form of monies that could be stolen from accounts or misuse of credit) that was at issue in *Krottner* and cases that follow it post-*Clapper*. *See Krottner*, 628 F.3d at 1142–43; *In re Adobe Sys.,*

[38] Motion to Dismiss – ECF No. 166 at 13–24.

> *Inc. [Privacy Litig.]*, 66 F. Supp. 3d [1197,] 1214 [(N.D. Cal. 2014)] (names, usernames, passwords, email addresses, phone numbers, mailing addresses, and credit-card numbers and expiration dates); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 955–57 (S.D. Cal. 2014). At oral argument, Mr. Antman's attorney asserted that harm can come from the misappropriation of a name and a driver's license. The court cannot reach that conclusion based on this complaint's allegations. To the extent that Mr. Antman asserts more in his declaration, the court does not consider the declaration and considers only the pleadings, judicially noticed facts, and documents incorporated by reference.
>
> Given this holding, mitigation expenses do not qualify as injury; the risk of identity theft must first be real and imminent, and not speculative, before mitigation costs establish injury in fact. *See Krottner*, 628 F.3d at 1143; *see also In re Zappos.com, Inc.*, No. 3:12-cv-00325-RCJ-VPC, 2015 WL 3466943, at *10–11 (D. Nev. June 1, 2015); *Lewart v. P.F. Chang's China Bistro, Inc.*, No. 14-cv-4787, 2014 WL 7005097, at *3 (N.D. Ill. Dec. 10, 2014); *In re Adobe Sys., Inc.*, 66 F. Supp. 3d at 1217; *In re Barnes & Noble Pin Pad Litig.*, No. 12-cv-8617, 2013 WL 4759588, at *4 (N.D. Ill. Sept. 3, 2013).
>
> Mr. Antman also did not plead injury related to the delay; delay alone is not enough. *See Remijas [v. Neiman Marcus Grp., LLC]*, 794 F.3d [688,] 695 [(7th Cir. 2015)] ("delay in notification," on its own, "is not a cognizable injury" that confers Article III standing on a plaintiff) (citing *Price v. Starbucks Corp.*, 192 Cal. App. 4th 1136, 1143 (2011)); *In re Adobe Sys.*, 66 F. Supp. 3d at 1217–18 (concluding that the plaintiffs had not established Article III standing for their claim under California Civil Code § 1798.82 based on the defendant's alleged failure to reasonably notify them of the data breach because the plaintiffs did "not allege that they suffered any incremental harm as a result of the delay").

Id. at 16–17. The court also held that Mr. Antman did not plausibly plead that Uber's conduct caused his injury:

> Mr. Antman also has not plausibly alleged that Uber's conduct caused his injury. Article III requires "a causal connection between the injury and the conduct complained of—the injury has to be 'fairly . . . trace[able] to the challenged action of the defendant, and not . . . th[e] result [of] the independent action of some third party not before the court.'" *Lujan*, 504 U.S. at 560–61 (quoting *Simon v. E. Ky. Welfare Rights Org.*, 426 U.S. 26, 41–42 (1976)) (ellipses in original). Mr. Antman specifies disclosure only of his name and drivers' license information. It is not plausible that a person could apply for a credit card without a social security number; indeed, it is not disputed that one was used to apply for the Capitol One credit card. Mr. Antman alludes to the disclosure of unspecified "other personal information;" this is insufficient, and Mr. Antman has the burden of establishing the court's jurisdiction.

Id. at 17.

The new fact allegation in the SAC is that Mr. Antman's "banking information" was disclosed

in the Data Breach.[39] At the hearing, however, Mr. Antman's counsel said that he did not know what the disclosed "banking information" was.[40] Uber's counsel countered that (1) Uber told Mr. Antman what "banking information" was disclosed, (2) the term "banking information" has a defined meaning under the California statutes, (3) "banking information" is in the PII realm only when account access is enabled (such as with a credit-card number and the credit-card code or a bank-account number and a bank-account pin), and (4) that was not the "landscape" here and nothing scraped could be used in any kind of ID theft of the named plaintiffs.[41] While the court of course is confined to the allegations in the complaint, Mr. Antman's counsel offered no alternate definition as to what was meant when Mr. Antman pleaded that his "banking information" was disclosed,[42] and hence the court reads the SAC through that lens.

Uber contends that Mr. Antman does not plead a credible threat of ID theft based on stolen data because the "banking information" that was stolen is not of the kind that can be used to access financial accounts.[43] Mr. Antman did not allege that the breached database contained his banking password, his PIN, his Social Security number, or other information that an ID thief could use.[44] To be fair, Mr. Antman did allege that his Social Security number and other PII have been made available for sale on the "dark web."[45] But, notably, he did not allege that his Social Security number or other PII that an ID thief could use *were disclosed in the Data Breach*.[46] Absent such an allegation, Mr. Antman cannot plead a claim by saying only that "bank information" was scraped in the Data Breach. Bank information that is not linked to a password might not pose any threat of ID theft.

Given the conclusory allegation of "banking information," the court holds that Mr. Antman did

---

[39] SAC – ECF No. 163 at 6–7 (¶ 29).

[40] Reporter's Transcript ("RT") 11/2/2017 – ECF No. 174 at 13:6–7.

[41] *Id.* at 19:5–21:12.

[42] *See id.* at 13:6–7.

[43] Motion to Dismiss – ECF No. 166 at 9.

[44] *Id.* at 15 n.2, 21.

[45] *Id.* at 7 (¶ 30).

[46] *See id.*

not plausibly plead a credible threat of identity theft that risks real, immediate injury. *See id.* at 16 (summarizing cases holding that the risk is in the form of monies that could be stolen from accounts or misuse of credit) (citations omitted). Whatever PII Uber has for its drivers presumably came from the drivers, including banking information. Mr. Antman must say what it was and how he was harmed by its disclosure, else the court cannot conclude that Uber collected and stored PII that — if disclosed — plausibly risks identity fraud. *Cf. Attias v. Carefirst, Inc.*, 865 F.3d 620, 625–28 (D.C. Cir. 2017) (the complaint alleged that the health insurer CareFirst collected and stored PII that included credit-card and Social Security numbers, PII was stolen in the breach, and the cyberattack on CareFirst put the plaintiffs at a high risk of financial fraud). Given this holding, and for the reasons set forth in the court's earlier order, the mitigation expenses do not qualify as injury because the risk of identity theft must be real before mitigation can establish injury in fact. *Id.* at 16–17 (summarizing cases) (citations omitted).

Moreover, even if he plausibly pleads a credible risk of identity theft by the disclosure of "banking information," Mr. Antman still has not plausibly alleged that Uber's conduct caused his injury. Article III requires "a causal connection between the injury and the conduct complained of — the injury has to be 'fairly . . . trace[able] to the challenged action of the defendant, and not . . . th[e] result [of] the independent action of some third party not before the court.'" *Lujan*, 504 U.S. at 560–61 (quoting *Simon v. E. Ky. Welfare Rights Org.*, 426 U.S. 26, 41–42 (1976)) (ellipses in original). Mr. Antman specifies disclosure only of his name, driver's license information, and unspecified "banking information." As the court said in its earlier order, "[i]t is not plausible that a person could apply for a credit card without a social security number; indeed, it is not disputed that one was used to apply for the Capitol One credit card. Mr. Antman alludes to the disclosure of unspecified 'other personal information;' this is insufficient, and Mr. Antman has the burden of establishing the court's jurisdiction." Order – ECF No. 44 at 17.

The complaint alleges nothing about Mr. Link's PII. The allegations in the declaration establish only that his driver's license number and name were disclosed. These allegations do not establish a material risk of ID theft or causation, largely for the reasons set forth in the court's earlier order. *See id.* at 15–17.

In other cases that have gone forward, there were known data breaches of PII that plausibly risked ID theft, even if it was unknown whether a bad actor obtained the information. In *Krottner*, it was the laptop with employees' names, addresses, and Social Security numbers. 628 F.3d at 1140. In *Attias*, there was a data breach with PII that included credit-card and Social Security numbers. Here, by contrast, this many years later, the plaintiffs do not plausibly allege an immediate, credible risk of harm. *See In re Zappos.com*, 108 F. Supp. 3d 949, 957, 959 (D. Nev. 2015) ("Immediacy is a common theme . . . It is not enough that a credible threat may occur at some point in the future; rather, the threat must be impending.).

In sum, the named plaintiffs do not allege that they were personally injured or that there is any plausible risk of immediate harm. The court dismisses the case for lack of Article III standing.

CONCLUSION

The court grants the motion to dismiss, dismisses the complaint for lack of standing, and — at the plaintiffs' request[47] — grants leave to amend. The court is not certain that the plaintiffs can cure the complaint's deficiencies to plausibly allege an immediate, credible risk of ID theft. But given that the reason for the delay to date was in aid of settlement discussions, and given that there was a post-dismissal disclosure that at least some Social Security numbers were compromised, the court gives a final opportunity to amend. Uber presumably knows exactly what information was disclosed in the data breach for Mr. Antman and Mr. Link. The early-settlement process was meant to provide discovery akin to jurisdictional discovery so that the plaintiffs would not plead a case that was contrary to the actual, knowable facts.

The plaintiffs must file any amended complaint in 28 days. If they decide to nonetheless stand on the SAC because they cannot cure the deficiencies, they must notify the court. If they then want to pursue a fees motion, the court grants Uber's request for further briefing and directs the

[47] Opposition to Motion to Dismiss – ECF No. 168 at 22 (asking for leave to amend to add facts about Mr. Link and leave to amend generally). The Link allegations would not change the court's conclusion here. The point of the amendment is to allow a final opportunity to allege — based on what the plaintiffs know about PII that they gave Uber and the data breach itself — a real and imminent, and not speculative, risk of identity theft. *Krottner*, 628 F.3d at 1143; *Zappos*, 108 F.3d at 957.

plaintiffs to file any motion on the ordinary five-week schedule.[48]

This disposes of ECF No. 166.

IT IS SO ORDERED.

Dated: November 25, 2017

LAUREL BEELER
United States Magistrate Judge

United States District Court
Northern District of California

[48] Opposition to Motion to Dismiss – ECF No. 168 at 22; Reply – ECF No. 169 at 20.