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** Re: ECF No. 182

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 only by Mr. Antman — for lack of standing. *Antman v. Uber Techs., Inc.*, No. 3:15-cv-01175-LB,

[1] Third Amended Complaint ("TAC") – ECF No. 179 at 3 (¶¶ 6–8), 4 (¶¶ 13–14), 5 (¶¶ 18–19). Citations refer to material in the Electronic Case File ("ECF"); pinpoint citations are to the ECF-generated page numbers at the top of documents.

2015 WL 6123054, at *9–12 (N.D. Cal. Oct. 19, 2015) (*Antman I*). 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 that could be accessed — there was no plausible, immediate risk of fraud or identity theft. *Id.* at *11.[2]

The parties then engaged in informal discovery and tried (unsuccessfully) to mediate the dispute.[3] The plaintiffs filed their Second Amended Complaint ("SAC"), adding Mr. Link as a named plaintiff.[4] The court again dismissed the case for lack of Article III standing again because the plaintiffs did not plausibly allege any risk of immediate harm.[5] The plaintiffs filed a Third Amended Complaint ("TAC"), raising the same claims that were in the SAC: (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 ("UCL"), Cal. Bus. & Prof. Code § 17200; (3) negligence; and (4) breach of implied contract.[6] 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.[7]

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).[8] The court grants the motion and dismisses the complaint with prejudice.

---

[2] *Id.* at 16.

[3] Status Report – ECF No. 154.

[4] Second Amended Complaint ("SAC") – ECF No. 163.

[5] Order (*Antman II*) – ECF No. 175 at 12–14.

[6] TAC – ECF No. 179 at 22–31. The First Amended Complaint raised only the first two claims. *See* First Amended Complaint ("FAC") – ECF No. 7.

[7] TAC – ECF No. 179 at 23–31.

[8] Mot. – ECF No. 182 at 8–32.

STATEMENT[9]

The named plaintiffs are Sasha Antman and Gustave Link. Both worked as Uber drivers in California.[10] They sue for Uber's failure to protect their PII "including names, driver's license 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."[11]

1. The Data Breach

"Beginning in or around May 2014, a hacker or hackers utilized credentials that one or more of Defendant's employees made available via GitHub (a web-based app designed for sharing code among app developers) to access a database containing Defendant's drivers' Private Information (the 'Data Breach'). In other words, Defendant not only permitted all of the compromised Private Information to be accessible via a single password, but allowed that password to be publicly accessible via the internet."[12] "Defendant could have prevented this Data Breach. It appears that Defendant maintained the Private Information in unencrypted form, and that the hacker(s) were able to access it freely with a basic password."[13]

---

[9] Unless otherwise noted, the fact allegations in the Statement are from the TAC.

[10] TAC – ECF No. 179 at 3 (¶¶ 6–7).

[11] *Id.* at 4 (¶ 13).

[12] *Id.* at 5 (¶ 18).

[13] *Id.* at 7 (¶ 24). The plaintiffs amplify this point: "On information and belief, 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. As a result, Plaintiffs' and Class members' Private Information was compromised and stolen." *Id.* at 8 (¶ 25). "Unfortunately, Defendant's apparent approach at maintaining the privacy of Plaintiffs' and Class members' Private Information, which relied solely on a password, was lackadaisical, cavalier, reckless, or at the very least, negligent." *Id.* at 17 (¶ 68).

Uber disclosed the data breach on February 27, 2015 in a press release, set forth in whole here:

> 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 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.[14]

[14] *Id.* at 5–6 (¶ 20) (citing Wong Decl. – ECF No. 24-1 at 4–5). The court considers entire the press release under the incorporation-by-reference doctrine. *Knievel v. ESPN*, 393 F.3d 1068, 1076 (9th Cir. 2005).

"Contrary to Defendant's representations [in the press release]: (a) the Data Breach compromised Private Information of many more than 50,000 drivers; (b) more Private Information than drivers' license numbers and names was disclosed in the Data Breach, including Social Security Numbers and banking information; (c) there have been reports of misuse of information as a result of the Data Breach, including the allegations of this lawsuit; and (d) Defendant did not 'take seriously' its 'responsibility to safeguard personal information,' nor did it take steps to ensure that the same thing would not happen again — to the contrary, it continued to allow credentials sufficient to access such Private Information to be posted on GitHub where, as Defendant was aware, those credentials could be (and would be) accessed by unauthorized parties, and it continued to fail to ensure that the Private Information in its possession could not be accessed without such credentials (for instance, by employing commonly used multi-factor authentication access protocols and encryption)."[15]

At about the same time that it issued the press release, Uber issued notifications to victims of the data breach (including both named plaintiffs) with substantially the same information and informing them that their names and driver's license numbers were disclosed in the data breach.[16]

In August 2016 (after the court's October 2015 order dismissing the FAC), Uber "issued more notifications to victims of the Data Breach informing them that additional Private Information was disclosed in the Data Breach (the 'Second Breach Notification'), and offering another year of credit monitoring."[17] "In its Second Breach Notifications, Defendant revealed that, contrary to the initial representations concerning the scope of the Data Breach in its Press Release and at the time of the Court's ruling on Defendant's motion to dismiss, additional Private Information was disclosed in the Data Breach, including banking information and Social Security Numbers, in addition to driver's license numbers and names."[18]

---

[15] *Id.* at 6–7 (¶ 21).

[16] *Id.* at 7 (¶ 23).

[17] *Id.* at 8 (¶¶ 26–27).

[18] *Id.* (¶ 28). The plaintiffs allege on information and belief that the New York Attorney General's Office investigated the data breach in 2015 and discontinued the investigation "through an Assurance

(cont'd)

In October 2016, Uber had a second data breach, which was revealed in news reports on November 21, 2017: "the Private Information of some 57 million of Defendant's riders and drivers was accessed by hackers (the '2016 Data Breach')."[19] Uber paid $100,000 to the hackers to cover up the breach instead of notifying victims.[20] "According to the news reports, the 2016 Data Breach occurred when two hackers 'accessed a private GitHub coding site used by Uber software engineers and then used login credentials they obtained there to access data stored on an Amazon Web Services account that handled computing tasks for the company. From there, the hackers discovered an archive of rider and driver information. Later, they emailed Uber asking for money, according to the company.'"[21] "'GitHub said the attack did not involve a failure of its security systems. "Our recommendation is to never store access tokens, passwords, or other authentication or encryption keys in the code," that company said in a statement.'"[22]

As evidence of Uber's dishonesty and efforts to impede or obstruct lawsuits and government investigations, the plaintiffs cite the *Waymo v. Uber* trade-secrets lawsuit (and information revealed there), Uber's operation of a "Marketplace Analytics Team" that used encrypted, self-deleting communications systems, and Uber's behavior in another lawsuit in the Southern District

---

of Discontinuance executed by Defendant and the New York Attorney General's Office in January 2016, which was based, in part, on Defendant's representations to the New York Attorney General's Office that the Data Breach only compromised driver's license numbers capable of being matched to driver names — which turned out not to be true." *Id.* at 8–9 (¶ 29). The plaintiffs allege on information and belief that Uber "notified the New York Attorney General that additional Private Information was disclosed in the Data Breach around the same time it issued the Second Breach Notifications, in accordance with New York law, and at that time stated that it was issuing the Second Breach Notifications because of information Defendant discovered as a result of the investigation it conducted in connection with this action." *Id.* at 9 (¶ 30).

[19] *Id.* at 10 (¶ 33) (citing Eric Newcomer, *Uber Paid Hackers to Delete Stolen Data on 57 Million People*, Bloomberg, Nov. 21, 2017, *available at* https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data).

[20] *Id.* (¶¶ 34–37) (quoting Newcomer).

[21] *Id.* at 11 (¶ 39).

[22] *Id.* (¶ 40) (quoting Joseph Menn & Dustin Volz, *Uber Paid 20-Year-Old Florida Man to Keep Data Breach Secret*, Reuters, Dec. 6, 2017, *available at* https://www.reuters.com/article/us-uber-cyber-payment-exclusive/exclusive-uber-paid-20-year-old-florida-man-to-keep-data-breach-secret-sources-idUSKBN1E101C).

of New York.[23] The plaintiffs allege that Uber's representations about the scope of the data breach in its notifications and filings cannot be trusted.[24] Even if Uber's representations about the scope of the breach are true, "disclosure of the types of Private Information that Defendant admits were compromised presents a danger to victims. Information such as data breach victims' names, birth dates, email addresses, and other identifying information alone creates a material risk of identity theft. Identity thieves can use such Private Information to locate additional Private Information, such as financial information and Social Security Numbers, and use the combined information to perpetrate fraud such as, for instance, opening new financial accounts in victims' names, or filing false tax returns in victims' names and collecting the tax refunds."[25]

The plaintiffs want discovery to permit their expert to examine the forensic data and to find a suitable class representative (apparently because the named plaintiffs do not allege that their Social Security numbers were disclosed).[26]

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."[27] Mr. Antman "received a First Breach Notification from Defendant 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."[28] The notice is attached as Exhibit A to the TAC, tracks the information in the press release (summarized above), and notified Mr. Antman that someone accessed one of Uber's databases once on May 13, 2014 and that the database had Mr.

[23] *Id.* at 11–12 (¶¶ 41–44).
[24] *Id.* at 23 (¶ 46).
[25] *Id.* at 13–14 (¶ 48) (emphasis removed).
[26] *Id.* at 14 (¶¶ 49–50).
[27] *Id.* at 15 (¶ 52).
[28] *Id.* (¶ 53).

Antman's name and driver's license number.[29] Mr. Antman "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."[30] The notice is attached as Exhibit B to the TAC and notifies Mr. Antman that — among other things — his "name, bank account and routing number were contained in the database."[31]

"On or around June 2, 2014, an unknown and unauthorized person used Plaintiff Antman's Private Information to apply for a credit card with Capital One, which now appears on [his] credit report."[32] "Plaintiff Antman spent significant time attempting to file a police report concerning this fraud, and working with banks and credit bureaus to secure his financial accounts against additional attempts to commit fraud against him, including by placing fraud alerts and freezes on his credit file. He subsequently experienced difficulty in obtaining new credit, obtaining financing for the purchase of a home, and noticed a stark decrease in the number of offers he receives for credit."[33]

Mr. Link worked as an Uber driver in the San Francisco Bay Area from approximately August 2012 until January 2015.[34] He "received a First Breach Notification from Defendant in or around March 2015, notifying him for the first time that his Private Information was disclosed in the Data Breach."[35] "In August 2015, after the Data Breach, the IRS rejected Plaintiff Link's tax filing for

---

[29] TAC Ex. A – ECF No. 179-1 at 2–3. As discussed in the initial press release, *see supra*, Uber offered a one-year credit-monitoring membership with Experian and a free credit report. *Id.*

[30] TAC – ECF No. 179 at 15 (¶ 54).

[31] TAC Ex. B – ECF No. 179-1 at 5–8. As discussed above, Uber offered an additional year's credit monitoring: "To help protect your identity, we are offering a complimentary one-year enrollment in My TransUnion Monitoring, a credit monitoring service provided by a subsidiary of TransUnion®, one of the three nationwide credit reporting agencies. This service helps detect possible misuse of your personal information, provides you with superior identity protection support focused on immediate identification and resolution of identity theft, and up to $1,000,000 in identity theft insurance with no deductible." *Id.* at 6.

[32] TAC – ECF No. 179 at 15 (¶ 55).

[33] *Id.* (¶ 56).

[34] *Id.* (¶ 57).

[35] *Id.* at 15–16 (¶ 58).

the December 31, 2014 tax period. Mr. Link learned this was the result of fraud, which occurred when someone used his PII to file a fraudulent tax return in his name, and to collect his tax refund, all before Plaintiff Link attempted to file his taxes. As a result, Plaintiff Link was forced to re-file his taxes and wait over eight months to receive his 2014 tax refund."[36]

> 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.[37]

Uber's breach 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."[38] "In addition, Plaintiffs spent significant time addressing the Data Breach (*see, e.g.*, ECF No. 30-1, Declaration of Sasha Antman)."[39]

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."[40] "Furthermore, Plaintiffs and other Class members were injured because they did not receive the benefit of the bargain entailed in the implied contracts between Plaintiffs and Defendant concerning security of their Private Information."[41]

---

[36] *Id.* at 16 (¶ 59).
[37] *Id.* (¶ 60).
[38] *Id.* (¶ 61).
[39] *Id.* (¶ 62).
[40] *Id.* (¶ 63).
[41] *Id.* (¶ 64).

The next section of the complaint is titled "The Stolen Private Information Is Valuable to Hackers and Thieves and Its Disclosure Harms Class Members."[42] It includes the following allegations about harm:

> 65. It is well known and the subject of many media reports that Private Information like that taken in the Data Breach at issue is highly coveted and a frequent target of hackers.
>
> 66. Legitimate organizations and the criminal underground alike recognize the value in such Private Information. Otherwise, they wouldn't pay for it or aggressively seek it.
>
> 67. "Increasingly, criminals are using biographical data gained from multiple sources to perpetrate more and larger thefts." Verizon 2014 PCI Compliance Report [link to report omitted].
>
> . . . .
>
> 70. The information compromised, including Class members' identifying information, is "as good as gold" to identity thieves, in the words of the Federal Trade Commission ("FTC"). . . .
>
> 71. The exposure of Plaintiffs' and Class members' Social Security numbers in particular poses serious problems. Criminals frequently use Social Security numbers to create false bank accounts, file fraudulent tax returns, and incur credit in the victim's name. Neal O'Farrell, a security and identity theft expert for Credit Sesame calls a Social Security number "your secret sauce," that is "as good as your DNA to hackers." [Citation omitted.] Even where data breach victims obtain a new Social Security number, the Social Security Administration warns "that a new number probably will not solve all [] problems . . . and will not guarantee [] a fresh start." [Citation omitted.] In fact, "[f]or some victims of identity theft, a new number actually creates new problems." One of those new problems is that a new Social Security number will have a completely blank credit history, making it difficult to get credit for a few years unless it is linked to the old compromised number.
>
> . . . .
>
> 73. As the FTC recognizes, once identity thieves have Private Information, they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance." [Citation omitted.]
>
> . . . .
>
> 76. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

[42] *Id.* at 16.

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm. [Citation omitted.]

77. Plaintiffs and Class members now face 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 that may be 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.[43]

4. Claims and 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.[44]

The first two claims are on behalf of a California class, defined as "[a]ll persons residing in California whose personal information was disclosed in the data breach affecting Uber Technologies, Inc. in 2014."[45] The third and fourth claims are on behalf of a national class or (in

[43] *Id.* at 16–20 (¶¶ 65–67, 70–73, 76–77).

[44] *Id.* at 23–31. For an analysis of the requirements of Cal. Civ. Code §§ 1798.81, 1798.81.5, and 1798.82, see the court's earlier order. *Antman I*, 2015 WL 6123054, at *5–6. 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; (4) medical information in the form of medical history, treatment, or diagnosis; or (5) health insurance information in the form of any unique identifier used by a health insurer to identify the individual (including insurance-policy number or subscriber-identification number) or any information in the individual's application and claims history. Cal. Civ. Code § 1798.81.5(d).

[45] TAC – ECF No. 179 at 21 (¶ 81).

the alternative) a California class. The national class is defined as "[a]ll persons residing in the United States whose personal information was disclosed in the data breach affecting Uber Technologies, Inc. in 2014."[46] 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 damages in claims three and four.[47]

LEGAL STANDARD FOR MOTIONS TO DISMISS

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. *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).

---

[46] *Id.* (¶ 80).

[47] *Id.* at 24–26 (¶¶ 102–05), 27–28 (¶¶ 116–17), 30 (¶ 128), 31 (¶ 139).

Standing pertains to the court's subject-matter jurisdiction and thus is properly raised in a Rule 12(b)(1) motion to dismiss. *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 which they rest. 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 matter, 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.* (citing *Twombly*, 550 U.S. at 556). "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) (internal quotation marks omitted).

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

1. Article III Standing

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 orders.[48] 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. *Antman I*, 2015 WL 6123054, at *10–11 (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

[48] Mot. to Dismiss – ECF No. 182 at 16–24.

> 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 *10. The court held that a credible threat of immediate identity theft based on stolen data is sufficient to establish injury in fact. *Id.* (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., 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 *11. 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.

The new fact allegation in the SAC was that Mr. Antman's "banking information" was disclosed in the Data Breach.[49] But Mr. Antman never specified what the disclosed "banking information" was.[50] The court concluded that Mr. Antman did not plausibly plead a credible threat of identity theft that risked real, immediate injury.[51]

> 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. 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." 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*. 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.[52]

The new fact allegation in the TAC is that Mr. Antman's "banking information" was his bank account and bank routing number.[53] The new allegation does not change the court's conclusion that the disclosed information does not plausibly amount to a credible threat of identity theft that

---

[49] SAC – ECF No. 163 at 6–7 (¶ 29).

[50] *Antman II* – ECF No. 175 at 11–13; Hr'g Tr. – ECF No. 174 at 13:6–7.

[51] *Antman II* – ECF No. 175 at 12–13.

[52] *Id.* at 12 (citing SAC – ECF No. 163 at 7 (¶ 30)).

[53] TAC – ECF No. 179 at 15 (¶ 54); TAC Ex. B – ECF No. 179-1 at 5.

risks real, immediate injury.[54] *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.[55]

Moreover, 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*, 426 U.S. at 41–42) (ellipses in original). Mr. Antman specifies disclosure only of his name, driver's license information, and his bank account and routing number. 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." *Antman I*, 2017 WL 6123054, at *11. The addition of the bank account and routing number to the fact allegations does not change this outcome: that disclosure did not cause the injury that Mr. Antman complains of.

Mr. Link also does not plausibly plead a credible threat of identity theft that risked real, immediate injury. The allegations in the TAC 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 for the reasons set forth in the court's earlier order. *Id.*

---

[54] *Antman II* – ECF No. 175 at 12–13 (citing *Antman I*, 2015 WL 6123054, at *11 (summarizing cases holding that the risk is in the form of monies that could be stolen from accounts or misuse of credit) (citations omitted)).

[55] *Id.* (citing *Antman I*, 2015 WL 6123054, at *11 (summarizing cases) (citations omitted)).

In other cases that have gone forward at the pleading stage, there were known data breaches of PII that plausibly risked fraud and 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. In *In re Zappos.com*, the information disclosed was "names, account numbers, passwords, email addresses, billing and shipping addresses, telephone numbers, and credit-card and debit-card information of more than 23 million Zappos customers." __ F.3d __, No. 16-16860, 2018 WL 1883212, at *2 (9th Cir. Apr. 20, 2018) (theft included customers' full credit-card numbers). Applying *Krottner* and its standard that the plaintiffs must allege "'a credible risk of real and immediate harm'" stemming from the theft of unencrypted personal data, the Ninth Circuit held in *Zappos* that "the information taken in the data breach still gave hackers the ability to commit fraud or identity theft, as Zappos itself effectively acknowledged by urging affected customers to change their passwords on any other account where they may have used 'the same or a similar password.'" *Id.* at *6 (quoting *Krottner*, 628 F.3d at 1143).

Here, by contrast, the plaintiffs do not allege a disclosure about their PII that plausibly suggests an immediate, credible risk of harm. The name, driver's license, and (for Mr. Antman) his bank account and routing information[56] do not plausibly risk fraud or identity theft for the reasons in the court's earlier orders. By contrast, fraud and identity theft are plausible risks with the account numbers and passwords disclosed in *Zappos*, the credit-card numbers and Social Security numbers in *Attias*, or the names, addresses, and Social Security numbers in *Krottner*.

The plaintiffs nonetheless allege that Uber's pattern of dishonesty means that it cannot be trusted.[57] Allegations about other lawsuits — and what they may or may not show about Uber's business practices — do not affect the court's inquiry. The court's inquiry is whether the plaintiffs

[56] This information is disclosed on the front of any check that a consumer writes, whether in hard copy or electronically. It is the way that money is routed.

[57] Mot. to Dismiss Opp'n – ECF No. 183 at 11–12.

plausibly plead that they were personally injured or that there is a plausible risk of immediate harm. The plaintiffs have not met this standard, and the court dismisses the case for lack of Article III standing.

2. Rule 12(b)(6)

Because the court dismisses the case for lack of Article III standing, the court addresses only perfunctorily Uber's motion to dismiss under Rule 12(b)(6).

First, as discussed in the last section, the plaintiffs fail to plead injury and causation. Actual injury is required for Uber's alleged failure to protect their PII under Cal. Civ. Code §§ 1798.81, 1798.81.5, and 1798.82. Cal. Civ. Code § 1798.84(b). The UCL claim also requires a party to show that he has "suffered injury in fact and has lost money or property as a result of the unfair competition." Cal. Bus. & Prof. Code § 17204; *see Rubio v. Capital One Bank*, 613 F.3d 1195, 1203–04 (9th Cir. 2010) (a plaintiff must sufficiently allege that (1) he has "lost 'money or property' sufficient to constitute an 'injury in fact' under Article III of the Constitution" and (2) there is a "causal connection" between the defendant's alleged UCL violation and the plaintiff's injury in fact) (citations omitted).

Second, if there is no predicate unlawful violation, there is no UCL "unlawful" claim. *Saunders v. Super. Ct.*, 27 Cal. App. 4th 832, 838–39 (1994); *see Farmers Ins. Exchange v. Super. Ct.*, 2 Cal. 4th 377, 383 (1992) (section 17200 "borrows" violations of other laws and treats them as unlawful practices independently actionable under section 17200 *et seq*.). And while a business practice may be "unfair or fraudulent in violation of the UCL even if the practice does not violate any law," *Olszewski v. Scripps Health*, 30 Cal. 4th 798, 827 (2003), the plaintiffs have not pleaded how Uber's acts were unfair or fraudulent.

Third, by not plausibly pleading injury and causation, the plaintiffs have not plausibly pleaded a negligence claim. *Merrill v. Navegar, Inc.*, 26 Cal. 4th 465, 500 (2001) (the elements of a negligence claim are (1) the existence of a duty to exercise due care, (2) breach of that duty, (3) causation, and (4) damages).

Fourth, the plaintiffs have not plausibly pleaded a claim for breach of an implied contract. They allege only this: "Furthermore, Plaintiffs and other Class members were injured because they did not receive the benefit of the bargain entailed in the implied contracts between Plaintiffs and Defendant concerning security of their Private Information."[58] They plead no facts about the existence of an implied contract, such as mutual assent and the other elements necessary to establish an express contract. *Northstar Fin. Advisors Inc. v. Shwab Inv.*, 779 F.3d 1036, 1050–51 (9th Cir. 2015); *Retired Emps. Ass'n of Orange Cty., Inc. v. County of Orange*, 52 Cal. 4th 1171, 1178 (2011) ("[A] contract implied in fact 'consists of obligations arising from a mutual agreement and intent to promise where the agreement and promise have not been expressed in words.'") (quoting *Silva v. Providence Hosp. of Oakland*, 14 Cal. 2d 762, 773 (1939)). Also, "it is well settled that an action based on an implied-in-fact or quasi-contract cannot lie where there exists between the parties a valid express contract [such as an Uber-driver agreement] covering the same subject matter." *Lance Camper Mfg. Corp. v. Republic Indem. Co.*, 44 Cal. App. 4th 194, 203 (1996) (citations omitted).

The court does not address Uber's other arguments given its dismissal for lack of standing.

CONCLUSION

The court dismisses the complaint without leave to amend. The issues have been the same in the three motions to dismiss. The court gave leave to amend, and the plaintiffs did not cure the complaint's deficiencies to plausibly allege an immediate, credible risk of fraud or ID theft.

If the plaintiffs want to pursue a fees motion, then the court grants Uber's request for further briefing.[59] The parties must confer within 14 days and settle on any briefing schedule.

IT IS SO ORDERED.

Dated: May 10, 2018

LAUREL BEELER
United States Magistrate Judge

[58] TAC – ECF No. 179 at 16 (¶ 64).

[59] Mot. to Dismiss Opp'n – ECF No. 183 at 28–29; Mot. to Dismiss Reply – ECF No. 187 at 20.