Tina Wolfson, SBN 174806
twolfson@ahdootwolfson.com
Robert Ahdoot, SBN 172098
rahdoot@ahdootwolfson.com
Theodore W. Maya, SBN 223242
tmaya@ahdootwolfson.com
AHDOOT & WOLFSON, PC
10728 Lindbrook Drive
Los Angeles, California 90024
Tel: 310-474-9111; Fax: 310-474-8585

Counsel for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

San Francisco Division

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

Plaintiff,

v.

UBER TECHNOLOGIES, INC., and DOES 1-50,

Defendants.

Case No. 3:15-cv-01175-LB

PLAINTIFFS' OPPOSITION TO DEFENDANT'S MOTION TO DISMISS THIRD AMENDED COMPLAINT

Third Amended Complaint Filed: Dec. 22, 2017

Hearing: April 19, 2018, at 9:30 a.m.
Dept.: Courtroom C, 15th Floor

Hon. Laurel Beeler, presiding

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

I. INTRODUCTION

Since the Court's last order dismissing this action on the pleadings, both the law and the facts have evolved such that Defendant's latest motion to dismiss must be denied.

With respect to the facts: While this case has been delayed by prior dismissal orders and by Defendant's game-playing at settlement negotiations, Defendant allowed another massive data breach to occur in a manner shockingly similar to the 2014 Data Breach at issue in this case. Instead of notifying victims of that 2016 breach about it, Defendant paid the hackers $100,000 in an attempt to cover up that breach, all while this case was pending. (Third Amended Complaint ("TAC") ¶¶ 33-40.)

With respect to the law: The Ninth Circuit recently handed down a controlling opinion making it clear that, contrary to Defendant's arguments, the risk of identity theft that resulted from Defendant's deficient cyber security practices, *alone*, constitutes a sufficient injury, resulting directly from the Data Breach, to satisfy Article III's standing requirements. Nevermind the actual instances of identity theft that both Plaintiffs allege resulted from the Data Breach. *See In re Zappos.com Inc., Customer Data Security Breach Litig.*, --- F.3d ----, 2018 WL 1189643 (9th Cir. March 8, 2018).

II. BACKGROUND

A. The 2014 Data Breach

Plaintiffs allege that Defendant Uber, the world's largest ride-hailing giant, failed to secure and safeguard its drivers' personally identifiable information including their names, driver's license numbers, banking information, Social Security Numbers, and other information (collectively, "Private Information"), and allege that Uber failed 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 was stolen, in a data breach that occurred in May 2014 (the "Data Breach," or the "2014 Data Breach").

This Data Breach occurred when a hacker or hackers utilized credentials that one or more 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, including names, driver's license numbers, banking information, Social Security numbers, and other personal identifying information. (TAC ¶ 18.) Defendant admitted that it knew of the Data Breach as early as

September 17, 2014, but chose not to disclose the Data Breach until February 27, 2015, when it issued a Press Release with representations concerning the Data Breach that later turned out to be more false than true. (TAC ¶¶ 18-19.)

Contrary to Defendant's representations in that 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). (*Id.* ¶ 21.)

At approximately the same time it issued its Press Release, Defendant also issued notifications to victims of the Data Breach, including to both Plaintiffs, informing them that their name and driver's license numbers were disclosed in the Data Breach (the "First Breach Notification"). (*Id.* ¶ 23.) However, "around August 2016" — over two years after the Data Breach — "Defendant 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." (*Id.* ¶ 27.)

Plaintiff Antman filed this action on March 12, 2015, and filed a First Amended Complaint a few days later, on March 16, 2015. (ECF 1, 7.) Defendant filed a motion to dismiss, which the Court granted on October 19, 2015. (ECF 44.) The Court encouraged Defendant to share information with Plaintiff's counsel during the hearing on that motion, and Defendant provided some limited information, but refused to engage in discovery and refuses to allow Plaintiffs' expert to examine the hacked databased to this day. (11/2/17 Tr. at 24.)

After the Court's October 19 order granting Defendant's Motion to Dismiss, the parties attempted to negotiate settlement, mediating with the Honorable Richard Kramer (Ret.) of JAMs. During that process, Defendant disclosed some information to Plaintiffs subject to the mediation privilege. As stated on the record by both parties, they reached agreement on a nationwide class action settlement, with the exception of a single issue. (TAC ¶ 31.)

Plaintiffs filed their Second Amended Complaint in July 2017, adding Plaintiff Link and a variety of allegations concerning the identity theft that both Plaintiffs suffered in the wake of the Data Breach. (ECF No. 163.) However, on November 25, 2017, the Court granted Defendant's motion to dismiss the Second Amended Complaint. In order to reach this conclusion, the Court accepted Uber's representations concerning the scope of the Data Breach. The Court reasoned that, because Plaintiffs did not allege that their banking password, PINs, Social Security numbers, "or other information that an ID thief could use" were disclosed in the Data Breach, Plaintiffs could not have Article III standing. (ECF No. 175 at 12.)

The Third Amended Complaint presently before the Court addresses the Court's concerns in a number of ways. First, it alleges that Defendant obtained and failed to protect a variety of highly sensitive "Private Information" belonging to Plaintiffs and other Class Members, including their Social Security Numbers. (TAC ¶ 13.) The TAC goes on to allege specific instances of identity theft Plaintiffs suffered and attribute to the Data Breach.

Mr. Antman received both a First and Second Breach Notification, while Mr. Link received only the First Breach Notification. (*Id.* ¶¶ 53-54, 58.) The TAC includes allegations regarding credit card fraud that Mr. Antman suffered in the wake of the Data Breach that required significant time for him to address, including by filing a police report and placing fraud alerts and freezes on his credit file. (*Id.* ¶¶ 55-56.) "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." (*Id.* ¶ 56.)

For his part, Plaintiff Link learned that someone filed a fraudulent tax return in his name "[i]n August 2015, after the Data Breach, [when] the IRS rejected Plaintiff Link's tax filing for the

December 31, 2014 tax period." (*Id.* ¶ 59.) "As a result, Plaintiff Link was forced to re-file his taxes and wait over eight months to receive his 2014 tax refund." (*Id.*)

Plaintiffs' investigation in connection with this case revealed that, "following the Data Breach[,] both Plaintiffs' Private Information, including their Social Security Numbers, have been made available for sale on the 'dark web.'" (*Id.* ¶ 60.) And Plaintiffs have not received notifications of other data breaches that might have compromised such information. (*Id.*)

In the TAC, Plaintiffs make clear that:

> even accepting Defendant's statements regarding the Data Breach as true, disclosure of the types of Private Information that Defendant admits were compromised in the Data Breach 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.

(TAC ¶ 48.)

B. <u>The 2016 Data Breach</u>

While the Court justifiably trusts Defendant's counsel (11/2/17 Tr. at 32-33), there is no basis for trusting Defendant itself when it says that Plaintiffs' Social Security numbers, as opposed to the Social Security numbers of other drivers, were not disclosed in the Data Breach. Putting aside the point that, as demonstrated in the argument section below and as alleged by Plaintiffs in the TAC, the risk of harm presented by the information Defendant *admits* was compromised, *alone*, conveys standing, the TAC includes a variety of allegations demonstrating that Uber is not to be trusted on such issues. Indeed, the fact that it waited so long to issue the First Breach Notifications, which then were proven woefully inadequate by the Second Breach Notifications, sufficiently makes this point.

As if its negligence in allowing the 2014 Data Breach to occur and its failure to notify victims about it were not enough, Defendant allowed another data breach to occur in the same manner as the 2014 Data Breach while this case was pending, but covered up that fact. On November 21, 2017 — days before the Court issued its November 25 Order dismissing Plaintiffs' Second Amended Complaint — news reports were published that Defendant suffered another, similar, massive data

breach in 2016, in which the Private Information of some 57 million Uber riders and drivers was accessed by hackers (the "2016 Data Breach"). (TAC ¶ 33.)

Defendant learned about the 2016 Data Breach by November 2016, but purposely chose not to notify those whose Private Information was compromised at that time; instead, Defendant paid the hackers who perpetrated it $100,000 in an effort to cover it up, and keep its victims ignorant about it. (*Id.* ¶¶ 35, 39.) Defendant thus conspired with the hackers who perpetrated the 2016 Data Breach to keep its victims — Defendant's drivers and riders — ignorant about it.

The 2016 Data Breach occurred in precisely the same manner as the 2014 Data Breach at issue in this case. According to 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, and later emailed Uber asking for money." (*Id.*)

C. Defendant's Conduct in Other Litigation

Defendant's conduct in other litigation underscores the point that its representations concerning the scope of the 2014 Data Breach should not be accepted at face value. In *Waymo LLC v. Uber Techs., Inc.*, No. 3:17-cv-00939-WHA (N.D. Cal. 2017), Judge Alsup concluded that he "can no longer trust the words of the lawyers for Uber in this case" after he was alerted to last-minute evidence, which ultimately forced him to delay trial in that case. (TAC ¶ 41.) That last-minute evidence involved a 37-page letter describing how Uber employees "implemented a sophisticated strategy to destroy, conceal, cover up and falsify records or documents with the intent to impede or obstruct government investigations as well as discovery obligations in pending and future litigation." (*Id.*) In that case, it was revealed that Defendant operated a shadowy "Marketplace Analytics Team" that utilized encrypted, self-deleting communications systems and, among other things "led efforts 'to evade, impede, obstruct, influence several ongoing lawsuits against Uber.'" (*Id.* ¶ 42.) There is every reason to suspect that this action is among those obstructed in such manner.

This pattern of dishonesty is exemplified in yet another case, in which Defendant's use of "unlicensed private investigators to conduct secret personal background investigations of both the

plaintiff and his counsel" came to light in a civil action. (TAC ¶ 44 (qutoing *Meyer v, Kalanick*, 1:15-cv-09796-JSR, ECF No. 119 at 1 (S.D.N.Y. July 25, 2016).) There, Judge Rakoff sanctioned Defendant, observing that "the processes of justice before the Court require parties to conduct themselves in an ethical and responsible manner, and [Defendant's] conduct here fell far short of that standard." *Id.* (quoting *Meyer*, ECF No. 119 at 30).

And, while Defendant has suggested to this Court that the Data Breach at issue was perpetrated by a competitor, that competitor — Lyft — consistently has denied the allegation, and the IP address used to perpetrate the Data Breach cannot be linked to any employee working there. (TAC ¶ 45.) "Plaintiffs seek discovery including an order permitting their expert to examine the hacked database and forensic data surrounding the Data Breach. Defendant has refused to permit such discovery without a Court order allowing it, and indeed Defendant refused even to provide complete responses to Plaintiffs' requests for production." (*Id.* ¶ 49.)

For the reasons set forth below, Plaintiffs respectfully request that Defendant's Motion to Dismiss the TAC (ECF 182, "Mot.") be denied in its entirety.

III. ARGUMENT

A. Both Plaintiffs Have Article III Standing

To demonstrate Article III standing, a plaintiff must show that she or he (1) "has suffered an 'injury in fact' that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." *In re Zappos.com Inc., Customer Data Security Breach Litig.*, --- F.3d ----, 2018 WL 1189643, *2 (9th Cir. March 8, 2018) (quoting *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 180-81 (2000); citing *Spokeo, Inc. v. Robins*, —— U.S. ——, 136 S.Ct. 1540, 1547 (2016)). "'A plaintiff threatened with future injury has standing to sue "if the threatened injury is "certainly impending," or there is a "substantial risk that the harm will occur."'" *Zappos*, 2018 WL 1189643, at *2 (quoting *Susan B. Anthony List v. Driehaus*, —— U.S. ——, 134 S.Ct. 2334, 2341 (2014), and *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 & n.5 (2013)).

1. Both Plaintiffs Allege Injury-in-Fact

a. The Risk of Future Harm, Alone, Constitutes Adequate Injury-in-Fact

In *Zappos*, the Ninth Circuit recently reversed dismissal of plaintiffs' claims in a data breach case, where those plaintiffs did not allege they had suffered any identity theft as a result of the data breach, which occurred in 2012. *Zappos*, 2018 WL 1189643, at *1. The court held that the risk of future injury "based on the hacking incident itself, not any subsequent illegal activity," was sufficient to satisfy Article III. *Id.*

Defendant bases much of its standing argument on a reading of *Clapper* that would require a future risk of injury to be "certainly impending" (Mot. at 12 (quoting *Clapper*, 568 U.S. at 409)), which ignores the fact that Article III standing also may be premised on a "'substantial risk'" of future harm, as the Ninth Circuit recognized in *Zappos* (relying in part on *Clapper*). *Zappos*, 2018 WL 1189643, at *2, 4. In this vein, Defendant invokes the "four years [that] have elapsed since the data breach of May 2014" (Mot. at 13 (citing, *inter alia*, the *Zappos* District Court opinion that the Ninth Circuit now has reversed)), but the data breach at issue in *Zappos* occurred in 2012 — even longer ago, and it concerned less sensitive information, particularly given that there were no allegations that the data breach in that case compromised Social Security numbers, as is the case here. *Id.* at *2, 5.

Not only does "[o]ur jurisdiction 'depend[] upon the state of things at the time of the action brought,'" *id.* at *5 (citation omitted), but Plaintiffs allege that the Private Information compromised in the Data Breach subjects them to risk for many years to come (TAC ¶¶ 51, 74, 76-77, 79). Moreover, the fact that Uber allowed another, very similar data breach to occur in 2016 weakens any force that its argument (that the passage of time since the 2014 data breach lessens the risk of harm) otherwise might have had. Defendant continues to negligently handle Plaintiffs' Private Information, and Plaintiffs seek injunctive relief to change that.

Under *Zappos*, the risk of future identity theft, alone, supports Plaintiffs' standing under Article III, regardless of whether Plaintiffs' Social Security numbers were compromised in the Data Breach. Accordingly, there is no need to engage in protracted analysis of whether the Private Information pertaining to Plaintiffs that Defendant admits was disclosed could have been used to

perpetrate the identity theft that both allege they suffered as a result of the Data Breach. Plaintiffs' allegations in that regard, however, are plausible and further support standing under Article III.

Much like Uber (Mot. at 15:23), the defendant in *Attias v. Carefirst, Inc.*, 865 F.3d 620, 628 (D.C. Cir. 2017), *cert denied* --- S.Ct. ----, 2018 WL 942459 (Feb. 20, 2018), argued that plaintiffs failed to allege that their Social Security numbers were compromised in a data breach and that, accordingly, they lacked standing. The Court of Appeal disagreed, because the plaintiffs alleged that the data breach in that case compromised a "category of 'PII/PHI/Sensitive Information,' as plaintiffs define it, [which] includes 'patient credit card . . . and social security numbers.'" *Id.* at 627 (ellipses in original). And, like *Zappos*, the *Attias* court reversed dismissal of plaintiffs' claims, reasoning that plaintiffs' allegations that their private information had been disclosed in the data breach met Article III's injury-in-fact requirement for standing purposes, in light of the "substantial risk" of future injury presented. *Id.* at 626-27 (citation omitted). "[E]xperience and common sense," the court held, establish "that plaintiffs would face a substantial risk of identity theft if their social security and credit card numbers were accessed by a network intruder." *Id.* at 628 (citation omitted).

Similarly here, Plaintiffs define "Private Information" as including Social Security numbers, which they specifically allege they provided to Defendant, and which Defendant admits were compromised in the Data Breach (although it contends that Plaintiffs' Social Security numbers were not compromised — a contested point of fact inappropriate for decision on a Rule 12 motion). (TAC ¶¶ 13, 15, 18, 21.) Although it is not necessary to find that Social Security numbers were disclosed in order to deny the present motion, the motion should not be granted on the basis that the TAC fails to plausibly allege that Plaintiffs' Social Security numbers were compromised in the Data Breach. Plaintiffs have alleged enough in that regard.

b. Plaintiffs' Alleged Identity Theft Also Constitutes Adequate Injury-in-Fact

In support of its argument that Plaintiff Antman's credit card fraud, and Plaintiff Link's delayed tax fraud, are not cognizable injuries, Defendant relies on *Whalen v. Michael Stores, Inc.*, 689 F. App'x 89 (2d Cir. 2017). (Mot. at 11-12.) As Judge Koh observed when defendant attempted to rely on *Whalen* in a data breach case before her:

> Defendants' reliance on *Whalen* is not persuasive. First, that case is an unpublished summary order from the Second Circuit, and it is accordingly not binding on this Court and indeed not binding in the Second Circuit itself. *See id.* (stating that rulings by summary order do not have precedential effect). Second, the facts alleged in *Whalen* are readily distinguishable from the instant case. The plaintiff in *Whalen* alleged that her credit card information was stolen in a data breach, and that her credit card was subsequently "physically presented for payment" in Ecuador on two occasions. *Id.* at *1. However, the plaintiff in *Whalen* "cancelled her card," and she did "not allege that any fraudulent charges were actually incurred on the card" or that "she was in any way liable on account of these presentations" of her credit card in Ecuador. *Id.* at *1. The Second Circuit affirmed the district court's dismissal of the complaint for lack of Article III standing because Whalen never alleged that fraudulent charges were actually incurred on her credit card, she never alleged a plausible threat of future fraud "because her stolen credit card was promptly cancelled," and Whalen did not allege that any other information—such as her birth date or Social Security number—was taken in the breach. *Id.* Moreover, Whalen did not allege "any time or effort that she herself has spent monitoring her credit." *Id.* Thus, the Second Circuit held that Whalen did not adequately allege that the data breach caused Whalen to suffer any injury that was concrete and particularized. *Id.*

In re Yahoo! Inc. Consumer Data Security Breach Litig., No. 16-MD-02752-LHK, 2017 WL 3727318, *15 (N.D. Cal. Aug. 30, 2017). The *Yahoo!* court went on to distinguish the facts before it on the basis that, in the *Yahoo!* case, plaintiffs alleged that "hackers obtained their Yahoo user names and passwords, dates of birth, credit and debit card account information, and/or Social Security number as a result of the Data Breaches, and that hackers used this information to steal benefits and/or to make a variety of fraudulent credit card charges and/or fraudulent tax filings in their names." *Id.*

As in the *Yahoo!* case, Plaintiffs' allegations of injury here go far beyond the attempted misuse of a single credit card that was alleged in *Whalen*, and Plaintiffs allege that the Data Breach compromised more sensitive Private Information that can be used to perpetrate identity fraud for years to come, whether or not a given credit card is cancelled.

Injuries resulting from fraudulent tax returns like Plaintiff Link's, including the time and expense incurred to resolve these issues with the IRS, readily satisfy the injury-in-fact requirement in data breach cases. *See, e.g.*, *Smith v. Triad of Alabama, LLC*, No. 1:14-CV-324-WKW, 2015 WL 5793318, at *9 (M.D. Ala. Sept. 29, 2015) (denying motion to dismiss where plaintiffs alleged fraudulent tax returns); *Longenecker-Wells v. BeneCard Servs., Inc.*, No. 1:15-CV-00422, 2015 WL 5576753, at *4 (M.D. Pa. Sept. 22, 2015) ("Confronted with the allegations that fraudulent tax returns

have already been filed in their names, we find that the other alleged injuries, or harms [which the court identified as "filing fees, accounting costs, and identity theft protection"], satisfy the 'injury-in-fact' prong to demonstrate standing to sue in the data-breach scenario we encounter here."). Many of the arguments Defendant asserts with regard to injury-in-fact are more properly understood as causation-based arguments, and those issues are addressed below.

c. Plaintiffs' Time and Effort Addressing and Protecting Against Identity Theft Also Constitutes Adequate Injury-in-Fact

As the Seventh Circuit held, "time and effort" a data breach victim reasonably expends in "monitoring both his card statements and his other financial information is "sufficient" to "support Article III standing." *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 965-69 (7th Cir. 2016); *see also In re Anthem, Inc. Data Breach Litig.*, MDL No. 2617, 2016 WL 3029783, at *26 (N.D. Cal. May 27, 2016) ("Plaintiffs' attempts to respond to this imminent threat—whether by paying out of pocket for credit monitoring or by using their own time for credit monitoring—resulted in damages that may be recoverable."); *Enslin v. Coca-Cola Co.*, 136 F. Supp. 3d 654, 665 (E.D. Pa. 2015) (holding that plaintiffs had standing where his credit cards or bank accounts had actually been misused by thieves because of a data breach for which defendant had responsibility).

d. Plaintiffs' Allege Injury-in-Fact in the Form of Loss of Value of Their Private Information

Plaintiffs further allege they suffered injury in fact in the form of loss of value of their Private Information. (TAC ¶ 63.) Plaintiffs allege that following the Data Breach, both Plaintiffs' Private Information, including their Social Security numbers, have been found available for sale on the "dark web," and that they know of no other source of such information besides the Data Breach at issue here. (*Id.* ¶ 60.)

The Ninth Circuit and a number of district courts have approved allegation of damages arising from the loss of value of PII. *In re Facebook Privacy Litigation*, 72 Fed.Appx. 494, 494 (9th Cir. 2014) (finding that plaintiffs plausibly alleged that they experienced harm where the plaintiffs' personal information was disclosed in a data breach, and the plaintiffs "los[t] the sales value of th[eir] personal information" as a result.); *see also, e.g.*, *Anthem*, 2016 WL 3029783, at *14-15 (finding that

plaintiffs plausibly alleged injury from the loss of value of their PII where the plaintiffs alleged that their PII was disclosed in a data breach, and that plaintiffs' PII was subsequently sold on the black market by hackers.); *Svenson v. Google, Inc.*, No. 13-cv-04080-BLF, 2015 WL 1503429, at *5 (N.D. Cal. Apr. 1, 2015) ("Svenson's allegations of dimunition of value of her personal information are sufficient to show contract damages for pleading purposes.").

In the *Yahoo!* case, Judge Koh similarly found injury in fact where plaintiffs alleged that "as a result of their valuable PII being for sale on the dark web, Plaintiffs have lost the value of their PII." *In re Yahoo!*, 2017 WL 3727318 at *14. Judge Koh explained: "Plaintiffs' allegations that their PII is a valuable commodity, that a market exists for Plaintiffs' PII, that Plaintiffs' PII is being sold by hackers on the dark web, and that Plaintiffs have lost the value of their PII as a result, are sufficient to plausibly injury arising from the Data Breaches." *Id.*

2. Plaintiffs' Alleged Injuries Are Fairly Traceable to the Data Breach

In addition to demonstrating that Plaintiffs here allege injury-in-fact to satisfy Article III, *Zappos* demonstrates that the injuries Plaintiffs allege are fairly traceable to the information that Defendant admits was compromised in the Data Breach (although, again, Plaintiffs do not believe Defendant can be trusted as to precisely what information was or was not disclosed in the Data Breach, and seek discovery on this issue). In *Zappos*, plaintiffs "allege[d] that the type of information accessed in the Zappos breach can be used to commit identity theft, including by placing them at higher risk of 'phishing' and 'pharming,' which are ways for hackers to exploit information they already have to get even more PII." *Zappos*, 2018 WL 1189643, at *13. The Ninth Circuit agreed with plaintiffs, concluding they had standing because, "[a]lthough there is no allegation . . . that the stolen information included social security numbers, . . . the information taken in the data breach still gave hackers the means to commit fraud or identity theft." *Id.*

Here, Plaintiffs allege that:

> even accepting Defendant's statements regarding the Data Breach as true, disclosure of the types of Private Information that Defendant admits were compromised in the Data Breach 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."

(TAC ¶ 48.)

Plaintiffs further allege that, "'[i]ncreasingly, criminals are using biographical data gained from multiple sources to perpetrate more and larger thefts.'" (TAC ¶ 67 (quoting Verizon 2014 PCI Compliance Report, available at <http://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_pci2014.pdf>, at 54 (last visited March 15, 2018)).) Not only do Plaintiffs allege that Defendant possessed and mishandled their Social Security numbers, but even the Private Information concerning Plaintiffs that Defendant admits was compromised presents sufficient risk to satisfy Article III's standing requirements.

Not only is the risk of future harm that Plaintiffs face as a result of the Data Breach fairly traceable to Defendant's wrongdoing, but the instances of actual identity theft they allege likewise meet Article III's causation requirement. Defendant wrongfully asserts that Plaintiff Antman somehow "admit[s] that the information exposed in the data breach was not the information used to apply for a credit card in his name." (Mot. at 12.) Similarly, Defendant erroneously states that Plaintiff Link fails to allege "allege the disclosure of any information other than his name and driver's license number." (*Id.* at 10.) In the TAC Plaintiffs clearly allege that they

> do not accept Defendant's current statements concerning the scope of the Data Breach . . . given: (a) the facts surrounding the 2014 and 2016 Data Breaches; (b) Defendant's knowingly reckless use of GitHub that repeatedly allowed credentials sufficient to access Plaintiffs' Private Information to be made available to hackers; (c) Defendant's repeated failure to secure Private Information in its possession in accordance with the law and sufficient to prevent such credentials, alone, to allow a hacker to access such Private Information; and (d) Defendant's pattern of false statements concerning those Data Breaches and concerning related issues before other courts, including its "efforts 'to evade, impede, obstruct, influence several ongoing lawsuits against Uber'"

(TAC ¶ 46.) And Plaintiffs allege they know of no other way, besides this Data Breach, that their Private Information — including Social Security numbers — could have been made available to identity thieves like those who preyed on them following the Data Breach. (TAC ¶ 60.)

There is no dispute that Defendant suffered a Data Breach, and that, as a result, Plaintiffs' Private Information was compromised. Defendant's failure to implement adequate safety measures to

protect drivers' information, and its failure to timely notify drivers about the Data Breach, clearly caused injuries to both Plaintiffs. *See also In re Yahoo!*, WL 3727318 at *18 (holding plaintiffs sufficiently alleged "a plausible 'casual chain' of events that links the Data Breaches, which [p]laintiffs allege resulted from Yahoo's failures to maintain appropriate data security measures, with the specific harms alleged by [p]laintiffs"); *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x, 384, 388 (6th Cir. 2016) ("[w]here a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in Plaintiffs' complaints."). Plaintiffs here allege that the stolen data was been made publicly available on the dark web, further implicating a concrete and impending risk of ID theft in the future. *Remijas v. Neiman Marcus Grp.*, LLC, 794 F.3d 688, 694 (7th Cir. 2015) ("[O]nce stolen data have been sold or posed on the Web, fraudulent use of that information may continue for years.").

Here, Plaintiffs allege, and Defendant does not dispute, that as a result of Defendant's failure to maintain adequate security measures, Plaintiffs' PII was compromised in the Data Breach, as confirmed by the fact that both Plaintiffs received notifications of the Data Breach. There is no justification to assume that the information disclosed in the Data Breach did not aid the identity thieves who committed fraud on Plaintiffs. There also is no justification to assume that the "banking information" that Uber admits was disclosed about Plaintiff Antman did not aid the identity thief who attempted to open an account in Plaintiff Antman's name, and there is no justification to assume that the information disclosed in the Data Breach played no role in the tax fraud that Plaintiff Link suffered in 2015. Following the Data Breach, both Plaintiffs received notifications of the Data Breach, and neither Plaintiff has received notification that similar information had been disclosed as a result of some other data breach. It is therefore plausible that this Data Breach is the cause of the loss of confidentiality and exposure to the risk of identity theft that Plaintiffs have suffered. Based on their allegations, Plaintiffs sufficiently allege that the risk of future harm they face is "fairly traceable to the conduct being challenged" —Uber's failure to prevent the Data Breach. *Zappos*, 2018 WL 1189643, at *16 ("That hackers might have stolen Plaintiffs' PII in unrelated breaches, and that Plaintiffs might suffer identity theft or fraud caused by the data stolen in those other breaches (rather than the data stolen from Zappos), is less about standing and more about the merits of causation and damages.").

3. Plaintiffs' Injuries Are Redressable by a Favorable Decision

As in *Zappos*, "[i]f Plaintiffs succeed on the merits, any proven injury could be compensated through damages. . . . And at least some of their requested injunctive relief would limit the extent of the threatened injury by helping Plaintiffs to monitor their credit and the like." *Zappos*, 2018 WL 1189643, at *7 (citing *Remijas*, 794 F.3d at 696-97).

B. Plaintiffs Adequately Plead All of Their Claims

In ruling on a motion to dismiss under Rule 12, the court analyzes the complaint and takes "all allegations of material fact as true and construe[s] them in the light most favorable to the nonmoving party." *Parks Sch. of Bus. v. Symington*, 51 F.3d 1480, 1484 (9th Cir. 1995). Ultimately, the Court may not dismiss a complaint in which the plaintiff has alleged "sufficient factual matter… to 'state a claim that is plausible on its face.'" *Ashcroft v. Iqbal*, 129 S.Ct. 1937, 1949 (2009).

1. Defendant's Inadequate Security and Delayed Notifications Violate California's Data Breach Act

Plaintiffs' claim under California's data breach act ("DBA"), Cal. Civ. Code §§ 1798.80 *et seq.*, is premised on: (1) Defendant's failure to "implement and maintain reasonable security procedures and practices appropriate to the nature of the" compromised Private Information, in violation of Cal. Civ. Code § 1798.81; and (2) Defendant's "fail[ure] 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," in violation Cal. Civ. Code § 1798.82. (TAC ¶¶ 92, 13.)

Defendant makes no argument that it complied with the DBA's requirements. Nor could it, given that Defendant failed to inform many drivers of the scope of the Data Breach that affect them for over two years following the Data Breach. (TAC ¶ 27.) During that time, Plaintiffs suffered the injuries complained of, including: Mr. Antman's credit card fraud and the time he spent addressing that; Mr. Link's delayed tax return; and both Plaintiffs' discovery that their Private Information was made available for sale on the "dark web." (TAC ¶¶ 55-60.) Had Defendant notified them of the Breach in a timely manner, they could have taken steps to prevent or, at least, minimize, these harms.

Just as Judge Koh found denied Adobe's motion to dismiss a DBA claim based on Adobe's failure to maintain reasonable security in *In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1217-19 (N.D. Cal. 2014), so too should this Court deny Uber's motion to dismiss here. Moreover, while the *Adobe* court dismissed the DBA claim based on delayed notification because plaintiffs in that case failed to allege harm resulting from the delay, the same cannot be said of the facts before this Court, and Defendant's motion should be denied in its entirety.

Defendant argues that Plaintiffs fail to allege actual injury under Cal. Civ. Code § 1798.84(b), reasoning that since Plaintiffs have not alleged the level of harm required for Article III, they also have not alleged any "actual loss or damage" for a DBA claim. (Mot. at 17-18.) Defendant's reliance on the unpublished decision in *Krottner v. Starbucks Corp.*, 406 F. App'x 129 (9th Cir. 2010), is misplaced given that *Krottner* did not consider a claim under the DBA or any statute, and dismissal of plaintiffs' tort claims were not supported by allegations of actual injury such as exist here.

Plaintiffs' allegations showing they suffered injury-in-fact for Article III standing, described above, also suffice for purposes of their DBA claim. *See Adobe*, 66 F. Supp. 3d at 1217 (finding plaintiffs' allegations of harm satisfied both Article III's requirements and supported their claim for violation of the DBA's requirement that defendant maintain "reasonable" security measures). Defendant's argument that the type of information disclosed in the breach is not actionable under the DBA is grounded on a contorted construction of the DBA, particularly in light of the fact that Uber itself failed to tell Plaintiffs what "banking information" was disclosed in the breach. That failure to disclose is, in and of itself, a violation of the DBA. Cal. Civ. Code § 1798.82(d)(2) (requiring notices to describe the types of information disclosed in the data breach); *Adobe*, 66 F. Supp. 3d at 1219 (denying motion to dismiss).

2. Plaintiffs State a Claim under the UCL

a. Plaintiffs Lost Money or Property as a Result of Defendant's UCL Violations

To state a claim under California's UCL, a plaintiff must have "suffered injuries in fact and . . . lost money or property" as a result of the unfair competition. Cal. Bus. & Prof. Code § 17204. There are innumerable ways to make this showing, including, for example: (1) surrendering in a transaction more, or acquiring in a transaction less than he or she otherwise would have; (2) having a present or

future property interest diminished; (3) being deprived of money or property; or (4) being required to enter into a transaction, costing money or property, that otherwise would have been unnecessary. *In re Anthem Data Breach Litig.*, 162 F. Supp. 3d 953, 985 (N.D. Cal. 2016).

Here, Plaintiffs lost money and property supporting their UCL claims in that both Plaintiffs allege that they were required to spend a significant amount of time addressing unauthorized transactions as a result of the breach, ensuring their identities are protected and monitoring their identity and credit. (TAC ¶¶ 56, 59.) Such allegations constitute "economic injury" sufficient to support a UCL claim. *Witriol v. LexisNexis Grp.*, No. C05-02392 MJJ, 2006 WL 4725713, *6 (N.D. Cal. Feb. 10, 2006) (finding plaintiffs adequately alleged economic injury under California's UCL where plaintiffs alleged that they "incurred costs associated with monitoring and repairing credit" after a data breach); *Walters v. Kimpton Hotel & Restaurant Grp., LLC*, No. 16-cv-05387-VC, 2017 WL 1398660, *2 (N.D. Cal. Apr. 13. 2017) (finding plaintiff alleged economic injury sufficient to establish UCL standing where he alleged he was required to monitor his credit after the theft of his payment card data in a data breach); *see also In re Yahoo!*, 2017 WL 3727318, at *16 ("out-of-pocket mitigation expenses are . . . sufficient to allege injury in fact arising from [] Data Breaches."); *see also, e.g.*, *Attias*, 865 F.3d at 629 (holding that "self-imposed risk-mitigation costs" such as "'the cost of responding to the data breach, the cost of acquiring identity theft protection and monitoring, [and the] cost of conducting a damage assessment . . . *can* satisfy the redressability requirement, when combined with a risk of future harm that is substantial enough to qualify as an injury in fact."); *Remijas*, 794 F.3d at 694 ("An affected customer, having been notified by Neiman Marcus that her card is at risk, might think it necessary to subscribe to a service that offers monthly credit monitoring."); *Corona v. Sony Pictures Entm't, Inc.*, No 14-CV-09600, 2015 WL 3916744, *4 (C.D. Cal. June 15, 2015) (reasoning that "costs associated with credit monitoring, password protection, freezing/unfreezing of credit, obtaining credit reports, and penalties resulting from frozen credit" supported plaintiffs' claims in data breach case).

Indeed, in Plaintiff Antman's case, the fraudulent attempt to open a credit card in his name, now appears in his credit report. That in and of itself is sufficient for UCL purposes, as it is well-established that damage to credit supports a UCL claim. *See, e.g.*, *Izsak v. Wells Fargo Bank, N.A.*,

No. C 13-05362 SI, 2014 WL 1478711, at *5 (N.D. Cal. Apr. 14, 2014) ("Damage to credit is sufficient to be a loss of money or property [supporting a UCL claim].") (citing *Rubio v. Capital One Bank*, 613 F.3d 1195, 1204 (9th Cir. 2010)); *King v. Bank of Am., N.A.*, No. C-12-04168 JCS, ECF No. 16, 2012 U.S. Dist LEXIS 141963, at *24 (N.D. Cal. Oct. 1, 2012) (allegations of diminished credit score satisfy the UCL's standing requirement.); *Rex v. Chase Home Finance, LLC*, 905 F. Supp. 2d 1111, 1147 (C.D. Cal. 2012) ("[D]amage to credit" is a "loss of money or property" within the meaning of the UCL).

Defendant contends that "the loss of 'personal information,' such as Social Security numbers, does not constitute lost money or property under the UCL." (Mot. At 19.) Defendant, however, misstates Plaintiffs allegations. In particular, Defendant fails to take into account that both Plaintiffs do not allege the loss of Private Information in a vacuum. Instead, Plaintiffs allege that as a result of the breach, their Private Information already has been *misused*. Such allegations are sufficient to constitute lost money or property under the UCL.

b. Plaintiffs' Allegations Satisfy the Unlawful, Unfair, and Fraudulent Prongs of the UCL

The UCL provides a cause of action for business practices that are (1) unlawful, (2) unfair, or (3) fraudulent. Cal. Bus. & Prof. Code § 17200. Here, Plaintiffs allege that Defendant's inadequate cybersecurity practices, which allowed the "security key" to its drivers' PII to be made publicly accessible, and Uber's failure to inform affected drivers of the Data Breach in a timely manner, constitute unlawful and unfair conduct sufficient to state a claim for purposes of the UCL.

The "unlawful" prong of the UCL prohibits "anything that can properly be called a business practice and that at the same time is forbidden by law." *In re Yahoo!*, 2017 WL 3727318, at *23 (citation omitted). By proscribing "any unlawful" business practice, the UCL permits injured consumers to 'borrow' violations of other laws and treat them as unlawful competition that is independently actionable." *Id.*

Here, Plaintiffs allege that Defendant violated Cal. Civ. Code §§ 1798.81.5 and 1798.82 by failing to disclose that it does not enlist industry standard security practices, which render Defendant's app and services particularly vulnerable to data breaches. That failure to disclose constitutes an

unlawful business practice under the UCL, and nothing more is required. *See Adobe*, 66 F. Supp. 3d at 1226 (finding Plaintiffs adequately alleged a UCL claim under unlawful prong where plaintiff adequately alleged underlying DBA violation).

The "unfair" prong of the UCL creates a cause of action for a business practice that is unfair even if not proscribed by some other law. *In re Yahoo!*, 2017 WL 3727318, at *23 (quoting *Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal, 4th 1134, 1143 (2003)). In *Yahoo!*, plaintiffs alleged, among other things, that "[d]efendants knowingly failed to employ adequate safeguards to protect their customers' data, in violation of [d]efendant's Privacy Policy, . . . and violated the policy of various California statutes . . . that were intended to 'reflect California's public policy of protecting consumer data." *In re Yahoo!*, 2017 WL 3727318, at *24. The court found plaintiffs' allegations sufficient "to allege that [d]efendant's conduct violated the balancing test," which weighs the utility of the defendant's conduct against the gravity of harm to the alleged victim. *Id.* It explained that plaintiffs "may proceed with a UCL claim under the balancing test by either alleging immoral, unethical, oppressive, unscrupulous, or substantially injurious conduct by [d]efendants *or* by demonstrating that [d]efendant's conduct violated an established public policy." *Id.*

Here, Plaintiffs' allegations are more egregious than those alleged by the plaintiffs in *Yahoo!*, and likewise are sufficient to state a claim under the UCL. *See also, e.g.*, *Anthem*, 162 F. Supp. 3d at 990 (finding plaintiffs adequately alleged unfair conduct under the balancing test where the complaint alleged that defendant failed to adequately protect customer data, which was allegedly in violation of several statutes that reflected California's public policy of protecting consumer data); *Adobe*, 66 F. Supp. 3d at 1227 (finding plaintiffs adequately alleged unfair conduct under the balancing test where plaintiffs alleged Adobe's conduct violated various data breach statutes that embodied California's public policy of protecting customer data); *Svenson*, 2015 WL 1503429, at *10 (finding plaintiffs sufficiently alleged violation of UCL's unfair prong where plaintiffs alleged that "Google violated its own privacy policies" by failing to safeguard the plaintiff's data).

In the cases on which Uber relies (*e.g.*, *Claridge v. RockYou, Inc.*, 785 F. Supp. 2d 855 (N.D. Cal. 2011) (cited in Mot. at 19)), plaintiffs attempted to premise their UCL claims on an alleged diminution or loss of value of their personal information, and did not allege they incurred any other

economic injuries as a result of defendants' conduct. These cases are distinguishable from the case at hand. Unlike the plaintiffs in the cases Uber cites, both named Plaintiffs here allege more than mere theft of their Private Information, and certainly more than mere speculation. Both Plaintiffs here allege the types of economic injuries consistently found sufficient to support a UCL claim, as demonstrated by cases like *Yahoo!*, which Defendant did not cite.

3. Plaintiffs State a Claim for Negligence

"To assert a negligence claim under California law, Plaintiffs must allege (1) the existence of a legal duty; (2) breach of that duty; (3) causation; and (4) a cognizable injury." *Corona*, 2015 WL 3916744, at *3 (citing *Paz v. State of California*, 22 Cal. 4th 550 (2000)).

Plaintiffs adequately set forth allegations supporting a negligence claim against Uber. Plaintiffs allege Uber violated its duty to safeguard Plaintiffs' PII by collecting and storing PII without adequate data security; Uber's breach of this duty proximately caused Plaintiffs to suffer harm; and this harm renders Plaintiffs' negligence claims plausible under California law.

Morevoer, California's economic loss rule does not apply where a "special relationship" exists between the parties. *Corona*, 2015 WL 3916744, at *5 (holding plaintiffs "sufficiently establish a special relationship that provides an exception to the economic loss doctrine" where they "were required to provide their PII to Sony" in order "to receive compensation and employment benefits"). Like *Corona*, because Plaintiffs had to provide their Private Information to Defendant in order to work as Uber drivers, a special relationship existed precluding application of the economic loss doctrine. *See also In re Experian Data Breach Litig.*, No. SACV 15-1592 AG, 2016 WL 7973595, at *8 (C.D. Cal. Dec. 29, 2016) (denying motion to dismiss negligence claim under California's Economic Loss Rule).

4. Plaintiffs State a Claim for Breach of Implied Contract

Plaintiffs allege that when Uber failed to reasonably protect their Private Information, and failed to timely notify Plaintiffs that their Private Information had been compromised, Uber breach its implied duty of good faith. Defendant argues that Plaintiffs have failed to adequately allege a contract in the first instance.

"An implied-in-fact contract requires proof of the same elements necessary to evidence an express contract: mutual assent or offer and acceptance, consideration, legal capacity and lawful subject matter." *Corona*, 2015 WL 3916744, at *6 (quoting *Northstar Financial Advisors Inc. v. Schwab Investments*, 779 F.3d 1036, 1050-51 (9th Cir. 2015) (citation omitted)).

Here, Plaintiffs allege that Uber offered employment to Plaintiffs in exchange for compensation and other benefits (TAC ¶¶ 15, 16.) It is implied in Plaintiffs' accepting Defendant's offer to drive for Uber that their information would be given for Defendant's use only. More importantly, drivers provided their Private information as a condition of their employment with Uber, and with the understanding that Uber would take adequate measures to protect it. (*Id.* ¶ 131.) Such actions constitute "an agreement between parties 'arrived at from their acts and conduct viewed in light of surrounding circumstances, . . . it grows out of the intentions of the parties to the transaction, and there must be a meeting of the minds." *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, No. 3:15-MD-2633-SI, 2017 WL 539578, at *16 (D. Or. Feb. 9, 2017) (citation and emphasis omitted).

By "providing their [s]ensitive information," and upon Defendant's acceptance of such information, the parties entered into implied-in-fact contracts for the provision of data security that obligated Uber "to take reasonable steps to secure and safeguard that information." *Id.*; *see also Smith v. Triad of Alabama*, No. 1:14-CV-324-WKW, 2017 WL 1044692, *5 (N.D. Ala. March 17, 2017) (certifying class in data breach case on claim for, *inter alia*, breach of implied contract); *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1176 (D. Minn. 2014) (holding that the plaintiffs sufficiently pleaded an "implied contract in which Plaintiffs agreed to use their credit or debit cards to purchase goods at Target and Target agreed to Plaintiffs' personal and financial information.").

When Uber failed to implement adequate safety measures to protect drivers' information and failed to notify drivers about a data breach, it breached this implied contract. Defendant cites *Careau & Co. v. Sec. Pac. Business Credit, Inc.*, 222 Cal App. 3d 1371, 1394 (1990) for the proposition that, under California law, establishing breach of an implied contract "requires proof a conscious and deliberate act that unfairly frustrates the agreed common purpose of the agreement." Uber argues that

its failure to safeguard Plaintiffs' information is plainly not a "conscious and deliberate act," which it claims, is required to establish a breach of implied contract.

While the rule in *Careau* has been followed by some federal district courts, it appears to be the minority position in California and is contradicted by more recent California Supreme Court authority. *See Carma Developers (Cal.) v. Marathon Dev. Col., Inc.*, 2 Cal. 4th 342, 373 (1992) ("Nor is it necessary that the party's conduct be dishonest . . . the covenant of good faith can be breached for objectively unreasonable conduct, regardless of the actor's motive."); *Neal v. Farmers Ins. Exchange*, 21 Cal. 3d 910, 921 n.5 (1978) ("The terms 'good faith' and 'bad faith' as used in this context are not meant to connote the absence or presence of positive misconduct of a malicious or immoral nature."). Moreover, the proposition that Uber's actions in making the security key necessary to access its drivers' PII were not "conscious and deliberate" involves an issue of fact that cannot be decided at the pleading stage.

Even if the Court follows *Careau*, Uber's conduct does not merely amount "an honest mistake, bad judgment, or negligence." (Mot. at 24.) To the contrary, Uber's actions are more aptly described as conscious and deliberate. Defendant offers no reason why it waited *five months* before issuing its press release or made any effort whatsoever to notify Plaintiff and other Class members of the breach, and *two years* before informing drivers that more sensitive Private Information in fact was disclosed in the Data Breach.

Defendant argues that Plaintiffs failed to show that they were harmed by Defendant's breach of the implied contract because Plaintiffs are in what Defendant refers to as "the same exact position as they had been had Uber safeguarded their PII." (Mot. at 24.) Defendant's assertions are contrary to the facts. Had Defendant "taken seriously" its "responsibility to protect Private Information," Plaintiffs' and class members' Private Information would never have been compromised — twice. Plaintiff Antman would not have suffered ID theft, and Plaintiff Link would not have suffered tax fraud. As a result of the Data Breach, Plaintiffs suffered a loss in value in their Private Information, and a loss of time and effort "sorting things out." *Remijas*, 794 F.3d at 692. They are not in the same position they would have been in if Defendant had employed reasonable cyber security and ensured that its employees did not place security credentials on GitHub or other insecure online environments.

C. Plaintiffs Should Be Permitted to Conduct Discovery

As alleged in the TAC, regardless of how the Court rules, Plaintiffs should be allowed an opportunity to conduct discovery to examine the hacked database and forensic data surrounding the Data Breach now. *CashCall, Inc. v. Superior Court*, 159 Cal. App. 4th 273, 284 (2008) ("Should the [trial] court conclude that the named plaintiffs may not adequately represent the class, it should afford them an opportunity to amend their complaint to redefine the class or to add new individual plaintiffs.' . . . . '[D]iscovery to ascertain a suitable class representative is proper.'") (quoting *Scott v. City of Indian Wells*, 6 Cal. 3d 541, 550 (1972), and *Best Buy Stores, L.P. v. Superior Court*, 137 Cal. App. 4th 772, 779 (2006) (citing *Budget Finance Plan v. Superior Court*, 34 Cal. App. 3d 794, 799 (1973) ("[I]f discovery is necessary in order to [afford a named plaintiff an opportunity to add new individual plaintiffs who adequately represent the class], it should be made available.")).

D. Plaintiffs Are Entitled to Seek an Award of Attorney Fees in Connection with the Second Breach Notifications

For all the reasons set forth in the preceding sections, Plaintiffs respectfully submit that Defendant's motion should be denied in its entirety. However, in the event the Court dismisses Plaintiffs' claims they request that, at a minimum, they be permitted to file a motion for attorney fees.

California Code of Civil Procedure § 1021.5 provides an exception to the general rule that each party to a lawsuit bear its own attorneys' fees. *Macdonald v. Ford Motor Co.*, 142 F. Supp. 3d 884, 890 (N.D. Cal. 2015). Under § 1021.5, a court may award attorneys' fees to a "successful party" when a lawsuit results in the enforcement of an important right affecting the public interest if (a) the enforcement creates a significant benefit for the general public or a large group of people; (b) the necessity and financial burden of enforcement make the award appropriate; and (c) the fees should not in the interest of justice be paid out of the plaintiff's recovery. Cal. Code Civ. Proc. § 1021.5.

A plaintiff does not have to win the lawsuit to be a "successful party." To obtain an award of attorneys' fees on a catalyst theory, "a plaintiff must establish that (1) the lawsuit was a catalyst motivating the defendants to provide the primary relief sought; (2) the lawsuit had merit and achieved its catalytic effect by threat of victory, not by dint of nuisance and threat of expense; and (3) plaintiffs

reasonably attempted to settle the litigation prior to filing the lawsuit." *Tipton-Whittingham v. City of Los Angeles*, 34 Cal. 4th 604, 608 (2004).

Where, after the plaintiff has sued, the defendant provides the relief the plaintiff seeks, the chronology of events may give rise to an inference that the litigation was a catalyst for the relief. *Edwards v. Ford Motor Co.*, No. 11CV1058-MMA (BLM), 2016 WL 1665793, at *5 (S.D. Cal. Jan. 22, 2016).

Plaintiffs allege that Defendant "notified the New York Attorney General . . . 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." (TAC ¶ 30.) Uber offered identity theft protection to the recipients of its Second Breach Notifications. (*Id.* ¶ 27.) In other words, this litigation already has conveyed a "significant benefit" to many Uber drivers meriting an award of attorney fees under California law. Cal. Code Civ. Proc. § 1021.5.

IV. CONCLUSION

For all the reasons explained above, Plaintiffs respectfully request that Uber's motion be denied in its entirety.

Respectfully Submitted,

Dated: March 15, 2018

AHDOOT & WOLFSON, PC

Tina Wolfson
Robert Ahdoot
Theodore W. Maya
10728 Lindbrook Drive
Los Angeles, California 90024
Tel: 310-474-9111
Fax: 310-474-8585

Counsel for Plaintiffs