UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

San Francisco Division

SASHA ANTMAN,

Plaintiff,

v.

UBER TECHNOLOGIES, INC.,

Defendant.

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

**ORDER GRANTING UBER'S MOTION TO DISMISS MR. ANTMAN'S FIRST AMENDED COMPLAINT**

[Re: ECF No. 24]

## INTRODUCTION

The plaintiff Sasha Antman filed this class-action lawsuit against the defendant Uber Technologies, Inc. ("Uber")—which operates a smart-phone mobile application connecting drivers and passengers—after an unknown hacker downloaded drivers' personal information (including drivers' names and license numbers) in May 2014, an event that Uber disclosed in February 2015. (*See* First Amended Complaint ("FAC"), ECF No. 7, ¶¶ 9-11.[1]). He raises two California statutory 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; and (2) unfair, fraudulent, and unlawful business practices, in violation of California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200. (*Id.* at 11-14.)

[1] Record citations are to documents in the Electronic Case File ("ECF"); pinpoint citations are to the ECF-generated page numbers at the tops of the documents.

United States District Court
Northern District of California

Uber moved to dismiss for lack of constitutional and statutory standing and for failure to state a claim. (Motion, ECF No. 24.) The court dismisses the First Amended Complaint without prejudice for lack of standing. Mr. Antman may file a Second Amended Complaint within 28 days from the date of this order.

## STATEMENT

Sasha Antman, who now lives in Oregon, previously worked as an Uber driver in San Francisco from an unspecified date until September 2013. (FAC ¶¶ 1, 18.) To use Uber's mobile application as Uber drivers, he and the putative class members gave Uber unspecified "personal information." (*Id.* ¶ 49.) The First Amended Complaint describes the personal information more granularly when describing the lawsuit: "Plaintiff brings this class action against Defendant for its failure to secure and safeguard its drivers' personally identifiable information including names, drivers['] license numbers, and other personal information ('PII') (collectively, 'Private Information')." (*Id.* ¶ 8.)

### I. THE DATA BREACH

"Beginning in or around May 2014, an unknown person or persons (the 'Hacker') utilized what [Uber] has described as a 'security key' to download files from [its] computer system containing its drivers' Private Information (the 'Data Breach')." (*Id.* ¶ 10.) "[T]he 'security key' used by the Hacker to perpetrate the Data Breach was publicly available on the internet via one or more GitHub webpages (and/or via the GitHub app, which is an app designed for sharing code among app developers)." (*Id.* ¶ 15.) "In other words, [Uber] not only permitted all of the compromised Private Information to be accessible via single password, but allowed that password to be publicly accessible via the internet." (*Id.*)

Uber did not disclose the Data Breach until February 27, 2015. (*Id.* ¶ 11.) On that date, Uber "disseminated a press release," which reads in its entirety as follows:

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

(Wong Decl., ECF No. 24-1, Ex. A; *see also* FAC ¶¶ 11-14. [2])

## II. HARM TO MR. ANTMAN

The complaint has a section titled "Plaintiff Was Damaged By the Data Breach." (FAC at 5.) In it, Mr. Antman alleges that on June 2, 2014, an unknown and unauthorized person used [his] Private Information to apply for a credit card with Capital One, which now appears on [his] credit report." (*Id.* ¶ 19.) Mr. Antman "received notification from [Uber] in or around March 2015,

[2] Generally, the court does not consider material beyond the pleadings in ruling on a motion to dismiss. *See United States v. Corinthian Colleges*, 655 F.3d 984, 998-99 (9th Cir. 2011). But the First Amended Complaint refers to and relies on Uber's February 27, 2015 press release and provides a link to it. (*See* FAC ¶¶ 11-14.) The court thus considers the entire press release under the incorporation-by-reference doctrine. *See Knievel v. ESPN*, 393 F.3d 1068, 1076 (9th Cir. 2005).

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." (*Id.* ¶ 20.) "[Uber's] notification to [him] did not include any explanation for the long delay in its issuance or indicate that the delay was due to any law enforcement investigation." (*Id.* ¶ 21.)

## III. HARM TO CLASS MEMBERS

The next section of the complaint is titled "The Stolen Private Information Is Valuable to Hackers and Thieves and Its Disclosure Harms Class Members." (*Id.* at 5.) It describes the value of personal identifying information to criminals engaging in identity theft. (*Id.* ¶¶ 22-30.) It notes the potential lag time between theft of personal identifying information and the use of it. (*Id.* ¶ 31.) It then describes the following harm to Mr. Antman and class members:

> 32. [Mr. Antman] 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 incurred by them and the resulting loss of use of their credit and access to funds, whether or not such charges are ultimately reimbursed by the credit card companies.
>
> 33. [Uber's] wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of [Mr. Antman's] and Class members' Private Information, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:
>
> a. theft of their Private Information;
>
> b. misuse of their Private Information such as the unauthorized attempt to open a credit card account in [Mr. Antman's] name described above, and additional such injury threatened in the future;
>
> c. damage to [Mr. Antman's] and Class members' credit reports and/or scores;
>
> d. the untimely and inadequate notification of the Data Breach;
>
> e. loss of privacy;
>
> f. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;
>
> g. deprivation of rights they possess under California law, including the Consumer Records Act and Business and Professions Code § 17200, et seq.
>
> 34. [Uber's] offer of one-year of free identity protection services, including credit monitoring, is insufficient compensation for damages resulting from [Uber's] actions and inactions because (a) that offer was made months after [Uber] learned of the breach, during which time [Mr. Antman's] and other Class members' Private Information was misused; (b) such credit monitoring does not prevent or retroactively

> fix the damage done to Class members and their credit reports; and (c) as the GAO reported, the PII could be held by criminals and used to commit fraud after the one year of credit monitoring and identity theft protection expires.

(*Id.* ¶¶ 32-34.)

**IV. RELIEF SOUGHT**

For the first claim, Mr. Antman seeks actual damages, attorney's fees, and costs; for the second claim, he seeks equitable relief (including restitution and disgorgement of fees Uber earned for rides); for both claims, he seeks the following injunction:

> an injunction requiring [Uber] to implement and maintain reasonable security procedures, including, but not limited to: (1) ordering that [Uber] utilize strong industry standard encryption algorithms for encryption keys that provide access to stored PII; (2) or ordering that [Uber] implement the use of its encryption keys in accordance with industry standards; (3) ordering that [Uber], consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests and audits on [Uber's] systems on a periodic basis; (4) ordering that [Uber] engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (5) ordering that [Uber] audit, test and train its security personnel regarding any new or modified procedures; (6) ordering that [Uber], consistent with industry standard practices, segment consumer data by, among other things, creating firewalls and access controls so that if one area of [Uber's] computer system is compromised, hackers cannot gain access to other portions of its systems; (7) ordering that [Uber] purge, delete, destroy in a reasonable secure manner customer data not necessary for its ongoing relationship with drivers; (8); ordering that [Uber], consistent with industry standard practices, conduct regular database scanning and security checks; (9) ordering that [Uber], consistent with industry standard practices, evaluate web applications for vulnerabilities to prevent web application threats to drivers; (10) ordering that [Uber], consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (11) ordering [Uber] to meaningfully educate its drivers and former drivers about the threats they face as a result of the loss of their Private Information to third parties, as well as the steps they must take to protect themselves.

(*Id.* ¶¶ 57, 59-60, 71.) He also asks the court to:

> require [Uber] to identify and notify all members of the Class who have not yet been informed of the Data Breach, and to notify affected drivers and/or users of its app of any future data breaches by email within 24 hours of [Uber's] discovery of a breach or possible breach and by mail within 72 hours.

(*Id.* ¶ 58.)

**GOVERNING LAW**

Uber moves to dismiss the complaint under (A) Federal Rule of Civil Procedure 12(b)(1) for lack of Article III standing and thus lack of federal subject-matter jurisdiction, (B) Rule 12(b)(6) for lack of statutory standing, and (C) Rule 12(b)(6) for failure to state a claim. This section sets forth the Rule 12(b) standards and the relevant California statutes.

## I. RULE 12(b)(1)

A complaint must contain a short and plain statement of the ground for the court's jurisdiction (unless the court already has jurisdiction and the claim needs no new jurisdictional support). Fed. R. Civ. P. 8(a)(1). The plaintiff has the burden of establishing jurisdiction. *See Kokkonen v. Guardian Life Ins. Co. of Am.*, 511 U.S. 375, 377 (1994); *Farmers Ins. Exchange 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). (If this were a factual challenge, the court would evaluate extrinsic evidence and resolve disputes when necessary; the plaintiff would have the burden of proving each requirement for subject-matter jurisdiction by a preponderance of the evidence. *Leitev. Crane Co.*, 749 F.3d 1117, 1121 (9th Cir. 2014).) A court may dismiss a complaint without leave to amend only if the complaint cannot be saved by amendment. *See Eminence Capital, LLC v. Aspeon, Inc.*, 316 F.3d 1048, 1052 (9th Cir. 2003).

## II. RULE 12(b)(6)

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

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

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

## III. THE CALIFORNIA STATUTES

The complaint has two 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; and (2) unfair, fraudulent, and unlawful business practices, in violation of California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200. (FAC, at 11-14.)

### A. California Civil Code §§ 1798.81, 1798.81.5 and 1798.82

California Civil Code § 1798.81.5 protects "personal information about California residents" by requiring business that "own, license, or maintain personal information about Californians to provide reasonable security for that information." Cal. Civ. Code § 1798.81.5(a)(1). "A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." *Id.* § 1798.81.5(b). The statute defines "personal information" as an individual's first name (or first initial) and last name with one or more of the following: (1) social security number; (2) driver's license number or California identification-card number; (3) account number or debit or credit card number in combination with the security code, access code, or password that permits access to that financial account, and (4) medical information in the form of medical history, treatment, or diagnosis. *Id.* § 1798.81.5(d).

Section 1798.81 requires a business to "take all reasonable steps to dispose, or arrange for the disposal, or customer records within its custody or control containing personal information when the records are no longer to be retained by the business by (a) shredding, (b) erasing, or (c) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means." "Customer" is defined as "an individual who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business [here, allegedly to use the Uber App to generate income as drivers]." *Id.* § 1798.80(c). (The claim is that Uber failed to dispose of Mr. Antman's personal information after he stopped working as an Uber driver, thus allowing his information to be compromised.)

Section 1798.82 has procedures for notifying California residences when their unencrypted personal information is disclosed in a data breach and thereby acquired by (or reasonably believed to have been acquired by) an unauthorized person. California Civil Code § 1798.82(a). The statute provides that the business "shall disclose" the breach and "shall notify" the affected persons. *Id.* § 1798.82(a)-(b). Notice can be delayed if a law-enforcement agency determines that notification will impede a criminal investigation; notification must be made promptly after the law-enforcement agency determines that disclosure will not compromise the investigation. *Id.* § 1798.82(c).

Section 1798.84(b) provides a private right of action: "[a]ny customer injured by a violation of this title may institute a civil action to recover damages." A business also may be enjoined. *Id.* § 1798.84(e). A prevailing plaintiff may recover his or her reasonable attorney's fees and costs. *Id.* § 1798.84(g).

### B. UCL Claim

California's Unfair Competition Law ("UCL") allows plaintiffs to bring claims for unfair, unlawful, or fraudulent business practices. Cal. Bus. & Prof. Code § 17200; *Guttierez v. Wells*

*Fargo Bank, NA*, 704 F.3d 712, 717 (9th Cir. 2012). Remedies under the statute are limited to injunctive relief and restitution. *Guttierez*, 704 F.3d at 717.

### ***1. "Unlawful" claim***

The "unlawful prong" of the UCL "incorporates other laws to make them actionable." *Jordan v. Paul Fin., LLC*, 745 F. Supp. 2d 1084, 1098 (N.D. Cal. 2010). "Generally, 'violation of almost any law may serve as a basis for a UCL claim.'" *Id.* (quoting in part *Plascencia v. Lending 1st Mortg.,* 259 F.R.D. 437, 448 (N.D. Cal. 2009) (citing in turn *Chabner v. United Omaha Life Ins. Co.*, 225 F.3d 1042, 1048 (9th Cir. 2000)). Claim one (asserting violations of Cal. Civ. Code §§ 1798.81, 1798.81.5, and 1798.82) is the predicate for the "unlawful" UCL claim, which stands or falls with claim one.

### ***2. "Fraud" claim***

To state a claim under the "fraud" prong of § 17200, a plaintiff must allege facts showing that members of the public are likely to be deceived by the alleged fraudulent business practice. *See Morgan v. AT&T Wireless Servs., Inc.*, 177 Cal. App. 4th 1235, 1255 (2009).

> The fraudulent business practice prong of the UCL has been understood to be distinct from common law fraud. A [common law] fraudulent deception must be actually false, known to be false by the perpetrator and reasonably relied upon by a victim who incurs damages. None of these elements are required to state a claim for injunctive relief under the UCL. This distinction reflects the UCL's focus on the defendant's conduct, rather than the plaintiff's damages, in service of the statute's larger purpose of protecting the general public against unscrupulous business practices

*Stearns v. Ticketmaster Corp.*, 655 F.3d 1013, 1020 (9th Cir. 2011) (quoting *In re Tobacco II Cases*, 46 Cal. 4th 298, 312 (2009). Named class representatives in UCL cases must still show "additional factors as to [themselves], such as injury in fact and causation." *Id.* at 1020 (citing *Tobacco II*, 46 Cal. 4th at 313-16). But absent members need not. *See id.*; *Tobacco II,* 46 Cal. 4th at 316 ("[T]he plain language of the [UCL] lends no support to the trial court's conclusion that all unnamed class members in a UCL class action must demonstrate section 17204 standing" by showing injury and causation.).

The "fraud" claim is based on Uber's security practices. "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, Defendant engaged in a fraudulent business practice that is likely to deceive a reasonable consumer." (FAC ¶ 68.) "A reasonable person would not have agreed to use the Uber app or to act as an Uber driver had he or she known the truth about Defendant's security practices. By withholding material information about Defendant's security practices, it was able to convince drivers and other users of its app to provide and entrust their Private Information to Defendant." (*Id.*¶ 69.)

#### ***3. "Unfair" claim***

A business practice can be unfair even if it is not unlawful. California courts have defined "unfair" business practices in several ways in consumer cases. *See Drum v. San Fernando Valley Bar Ass'n*, 182 Cal. App. 4th 247, 256 (2010). One of them is a business practice that "is immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers and requires the court to weigh the utility of the defendant's conduct against the gravity of the harm to the alleged victim." *Id.* (citing *Bardin v. Daimlerchrysler Corp.*, 136 Cal. App. 4th 1255, 1260–1261 (2006)); *Davis v. Ford Motor Credit Co.*, 179 Cal. App. 4th at 581, 595–596 (2009); *Gregory v. Albertson's Inc.*, 104 Cal. App. 4th 845, 854 (2002)). The FAC here relies on that theory: "Defendant's failure to disclose that it does not enlist industry standard security practices also constitutes an unfair business practice under the UCL. Defendant's conduct is unethical, unscrupulous, and substantially injurious to Class members." (*Id.* ¶ 70.)

## ANALYSIS

### I. REQUESTS FOR JUDICIAL NOTICE

Uber asks the court to judicially notice Uber's February 27, 2015 press release, a generic Capital One credit-card application obtained from Capital One's website on June 3, 2015, and the California Senate Committee on Privacy's Bill Analysis of AB 700. (Uber's RJN, ECF No. 25.) It also argues that the court can consider the press release and the credit-card application under the incorporation-by-reference doctrine. (*Id.* at 3-4.) Mr. Antman asks the court to judicially notice an opinion, *Remijas v. Neiman Marcus Group, LLC*, No. 14-3122 (7th Cir. July 20, 2015). (Mr. Antman's RJN, ECF No. 30-2.)

First, the court does not need to take judicial notice of the *Remijas* opinion or the legislative history because it can consider them without taking judicial notice of them. *See Von Saher v.*

*Norton Simon Museum of Art at Pasadena*, 592 F.3d 954, 960 (9th Cir. 2010) ("Judicial notice of legislative facts . . . is unnecessary.") (citing Fed. R. Evid. 201 advisory committee's note (1972)); *Toth v. Grand Trunk R.R.*, 306 F.3d 335, 349 (6th Cir. 2002) ("As a general matter, judicial notice is available only for 'adjudicative facts,' or the 'facts of the particular case,' as opposed to 'legislative facts,' which are facts 'which have relevance to legal reasoning . . . , whether in the formulation of a legal principle or ruling by a judge . . . or in the enactment of a legislative body.' Thus, judicial notice is generally not the appropriate means to establish the legal principles governing the case.") (quoting Fed. R. Evid. 201 advisory committee's note (1972))).

Second, the court does not take judicial notice of Uber's February 27, 2015 press release; instead—for the reasons set forth in note 2, *supra*—it considers the entire press release under the incorporation-by-reference doctrine. Finding that a document is incorporated by reference is different than judicially noticing a fact, *see Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 322 (2007); *Lee v. City of Los Angeles*, 250 F.3d 668, 688-89 (9th Cir. 2001), and the standards are different, too, *see Gammel v. Hewlett-Packard Co.*, 905 F. Supp. 2d 1052, 1061 (C.D. Cal. 2012). Federal Rule of Evidence 201 allows the court to "judicially notice a fact that is not subject to reasonable dispute because it: (1) is generally known within the trial court's territorial jurisdiction; or (2) can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned." Fed. R. Evid. 201(b). A "high degree of indisputability is the essential prerequisite" to taking judicial notice and "the tradition [of taking judicial notice] has been one of caution in requiring that the matter be beyond reasonable controversy." Fed. R. Evid. 201(a) & (b) advisory comm. nns. The court might be able to take judicial notice of the existence of the press release, but it does not take judicial notice of the facts within it (*e.g.*, that the Hacker accessed only drivers' names and license numbers) because those facts are not generally known within the court's jurisdiction, the press release is not a source whose accuracy cannot reasonably be questioned, and Mr. Antman objects to it.

Third, the court does not consider the credit-card application under the incorporation-by-reference doctrine or take judicial notice of it.

To the extent that Uber suggests that the court can consider the application under the incorporation-by-reference doctrine (*see* Uber's RJN, ECF No. 25 at 3-4), the court disagrees with Uber that the First Amended Complaint necessarily relies on the application; it refers only to an unauthorized person's application for a credit card in Mr. Antman's name, which is not the same as necessarily relying on this particular application. *See Knievel*, 393 F.3d at 1076.

The court also does not think that it can judicially notice the application. Mr. Antman asserts that it is "inappropriate to take judicial notice" to prove Uber's "contention that the criminal who attempted to open an account in Plaintiff's name used the credit card application . . . in order to perpetrate that fraud" and that "the criminal did not use Mr. Antman's Private Information disclosed in the Data breach to do so." (Objections to RJN, ECF No. 30-3 at 2.) Uber elaborates in its reply that the point of judicially noticing the application is that the data breach here is driver names and license numbers, and one also needs a social security number (as the application establishes) to apply for a credit card. (Reply, ECF No. 32 at 3.) The inference is that the injury (the application) had nothing to do with the data breach (only driver names and license numbers), which—if true—means that there is no case or controversy and no federal subject-matter jurisdiction. *See Susan B. Anthony List v. Driehas*, 134 S. Ct. 2334, 2341 (2014).

When a court takes judicial notice, often it is of the existence of public records and undisputed facts in them. *See Lee v. County of Los Angeles*, 250 F.3d 668, 689-90 (9th Cir. 2001). In a similar vein, courts take judicial notice of policy documents available on a government website. *See White v. Social Sec. Admin.*, No. 14-cv-05604-JST, 2015 WL 3902789, at *2 (N.D. Cal. June 24, 2015) (five Social Security Administration policy documents); *Gustavson v. Mars, Inc.*, No. 13-cv-04537-LHK, 2014 WL 2604774, at *3 n.1 (N.D. Cal. June 10, 2014) (Food and Drug Administration letters and press releases). Another example is taking judicial notice of another court's opinion to prove that evidence existed to put a party on notice of the facts underlying a claim. *See Sands v. McCormick*, 502 F.3d 263, 268 (3rd Cir. 2007). Key to these decisions is public availability and the undisputed reliability of the information in the documents.

These examples do not obviously answer the question of whether the court can take judicial notice of the publicly available credit-card application, a June 2015 application that has a temporal distance from the unauthorized application here in June 2014. (*See* FAC ¶ 19.). That said, needing a social security number to apply for a credit card—a fact made manifest by the website application—perhaps cannot be disputed reasonably. At oral argument, Mr. Antman's counsel said that it was undisputed that a social security number was used for the Capitol One application here. The court thus considers the need for a social security number in its evaluation of whether Mr. Antman plausibly alleged jurisdiction or his claims. The court need not (and does not) take judicial notice of the credit-card application itself.

## II. ARTICLE III STANDING

Uber first argues that Mr. Antman lacks Article III standing to pursue his claims.

"To establish Article III standing, a plaintiff must show (1) an 'injury in fact,' (2) a sufficient 'causal connection between the injury and the conduct complained of,' and (3) a 'likel[ihood]' that the injury 'will be redressed by a favorable decision.'" *Susan B. Anthony List v. Driehas*, 134 S. Ct. 2334, 2341 (2014) (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992)). "[E]ach element must be supported in the same way as any other matter on which the plaintiff bears the burden of proof, i.e., with the manner and degree of evidence required at the successive stages of the litigation." *Lujan*, 504 U.S. at 561. The court analyzes standing claim by claim. *California ex rel Imperial Cnty. Air Pollution Control Dist. v. U.S. Dep't of the Interior*, 77 F.3d 781, 789 (9th Cir. 2014) (citing *Lewis v. Casey*, 518 U.S. 343, 358 n.6 (1996)).

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).

The claims here turn on Uber's alleged failure to protect personal information of its drivers in violation of Cal. Civ. Code §§ 1798.81, 1798.81.5 and 1798.82. Uber argues that Mr. Antman did not plead injury in fact or a causal connection sufficiently. (Motion, ECF No 24, at 12-18.)

### A. Injury in Fact

"[T]he injury-in-fact requirement . . . helps to ensure that the plaintiff has a 'personal stake in the outcome of the controversy.'" *Driehaus*, 134 S. Ct. at 2341 (quoting *Warth*, 422 U.S. at 498). "An injury sufficient to satisfy Article III must be 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" *Id.* (quoting *Lujan*, 504 U.S.at 560) (internal quotation marks omitted). "An allegation of future injury may suffice if the threatened injury is 'certainly impending,' or there is a 'substantial risk that the harm will occur.'" *Id.* (quoting *Clapper v. Amnesty Int'l U.S.A.*, 133 S. Ct. at 1138, 1147, 1150 n.5 (2015) (internal quotation marks omitted)).

The allegations about injury are in a section of the complaint called "Plaintiff was damaged by the Data Breach." (FAC at 5.) The alleged injury occurred after a "criminal" used Mr. Antman's "'private Information [in June 2014] to apply for a credit card with Capital One Visa, which now appears on [his] credit report.'" (Opposition, ECF No. 30 at 9, citing FAC ¶ 19.) The complaint describes this later as an "unauthorized attempt to open a credit card in [his] name." (FAC ¶ 33(b).) Mr. Antman does not allege any fraudulent credit charges or loss of use of credit. Mr. Antman does refer—in the next section of the complaint titled "The Stolen Private Information Is Valuable to Hackers and Thieves and Its Disclosure Harms Class Members"—to the class's ongoing need to monitor credit and to "damage to Plaintiff's and Class Members' credit reports and/or scores." (*Id.* ¶¶ 32-33.) (At oral argument, his counsel included monitoring in his description of the injury.) As to Uber's failure to notify him promptly of the data breach, Mr. Antman complains that Uber did not tell him about the breach until March 2015, well after the data breach, and did not explain the delay. (*Id.* ¶¶ 20-21.) The private information disclosed was "names, drivers['] license numbers, and other personal information." (*Id.* ¶ 8.)

The harm thus is defined as an unauthorized application for a credit card and ongoing monitoring. The issue is whether these allegations establish injury in fact.

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

Uber nonetheless argues that a threat of harm resulting from a data breach is not sufficient post-*Clapper*. (Motion, ECF No. 24 at 12-15.) *Clapper* was a Foreign Intelligence Surveillance Act ("FISA") case involving the U.S. plaintiffs' "highly speculative fear" that (1) the government would decide to target communications of non-U.S. persons with whom the plaintiffs communicated, (2) the government would use its authority under the statute (rather than a different method of surveillance), (3) the Article III FISA judges would conclude that the government's proposed surveillance satisfied the statute's safeguards and was consistent with the Fourth Amendment, (4) the government would intercept communications of the plaintiffs' non-U.S. contacts, and (5) the plaintiffs would be parties to the intercepted communications. *See* 133 S. Ct. at 1148. That "speculative chain of possibilities" did not establish that injury based on potential future surveillance was "certainly impending" or fairly traceable to the FISA statute that the U.S. plaintiffs challenged. *Id.* at 1148-1150.

The court finds persuasive those cases that conclude that *Krottner* survives *Clapper*. The court thinks that a credible threat of immediate identity theft based on stolen data is sufficiently different than the speculative harm articulated in *Clapper*. *See Remijas v. Neiman Marcus Grp.*, 794 F.3d

United States District Court
Northern District of California

688, 693-94 (7th Cir. 2015); *In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp.3d 1197, 1212-14 (N.D. Cal. 2014). Moreover, the *Clapper* Court articulated an understandable reluctance to "decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional" or to "endorse standing theories that require guesswork as to how independent decisionmakers will exercise their judgment." 133 S. Ct. at 1147, 1150 (citations and quotations omitted). *Clapper* also involved a comprehensive scheme involving evaluation by the FISA court, required disclosures by the government, and other avenues of review. *Id.* at 1154. Identity theft does not implicate the kinds of issues that militated in favor of the *Clapper* Court's "rigorous" standing inquiry. *Id*. at 1147, 1150. Under *Krottner*, if the risk of identity theft is credible, real, and immediate, it is injury in fact that confers standing.

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.*, 66 F. Supp. 3d at 1214 (names, usernames, passwords, email addresses, phone numbers, mailing addresses, and credit-card numbers and expiration dates); *In re Sony Gaming Networks and 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*, 794 F.3d at 695 ("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").

### B. Causal Connection

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.

## III. STATUTORY STANDING

Uber moves to dismiss under Federal Rule of Civil Procedure 12(b)(6) for lack of statutory standing. (Motion, ECF No. 24 at 17-22.) *See Maya v. Centex Corp.*, 658 F.3d 1060, 1067 (9th Cir. 2011). California Civil Code § 1798.84(b) provides a private right of action: "[a]ny customer injured by a violation of this title may institute a civil action to recover damages." Mr. Antman did not allege a cognizable injury because he did not allege a causal connection between Uber's conduct and the credit-card application. He thus lacks statutory standing under section 1798.84(b) and the UCL. *See In re Adobe Sys.*, 66 F. Supp. 3d at 1218 (quoting and citing *Boorstein v. CBS Interactive, Inc.*, 222 Cal. App. 4th 456, 466-67 (2013)) (other citations omitted).

## IV. CALIFORNIA RESIDENCY

Another issue is that the California statutes that form the basis for claim one protect "personal information about California residents." Cal. Civ. Code § 1798.81.5(a)(1); *see also id.* § 1798.81.5(b). Mr. Antman was a California resident at the time he drove for Uber; he did not allege that he was one at the time of the data breach. If he was not, this may be an issue for claim one (which challenges Uber's alleged failure to maintain the reasonable security procedures required by the Civil Code); it may or may not be for claim two (the UCL claim), particularly with regard to the unfair or fraudulent UCL claims. Because Mr. Antman has not established his standing to bring the claims, and because the allegations in an amended complaint may affect the analysis, the court does not address this issue now.

## CONCLUSION

The court dismisses the First Amended Complaint without prejudice for lack of standing. Mr. Antman may file a Second Amended Complaint within 28 days from the date of this order. This disposes of ECF No. 24.

**IT IS SO ORDERED.**

Dated: October 19, 2015

LAUREL BEELER
United States Magistrate Judge