UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

PAUL DUGAS,

Plaintiff,

v.

STARWOOD HOTELS & RESORTS WORLDWIDE, INC., HST LESSEE SAN DIEGO, LP; HST GP SAN DIEGO, LLC,

Defendants.

Case No.: 3:16-cv-00014-GPC-BLM

ORDER GRANTING IN PART AND DENYING IN PART DEFENDANTS' MOTION TO DISMISS

[ECF No. 22]

Before the Court is Defendants Starwood Hotels and Resorts Worldwide, Inc. ("Starwood"), HST Lessee San Diego, LP, and HST GP San Diego, LLC's (collectively "Defendants") Motion to Dismiss. ECF No. 22. Upon review of the moving papers and the applicable law, and for the reasons set forth below, the Court **GRANTS** in part, without prejudice, and **DENIES** in part Defendants' Motion to Dismiss.

FACTUAL BACKGROUND

This case arises from a series of attacks by criminal hackers upon the United States hospitality industry. First Amended Class Action Complaint ("FACC"), ECF No. 21 ¶ 8. Plaintiff Paul Dugas ("Plaintiff") alleges that customer systems of Starwood Hotels and Resorts Worldwide, Inc. ("Starwood") had malicious software installed on them and that

they have been compromised since "at least November 2014." *Id.* ¶ 22. Plaintiff alleges that this data breach (the "Starwood breach") "adversely affected hundreds of thousands of customers of the Starwood Hotel system." *Id.* ¶ 4. According to Plaintiff, although Starwood "discovered the first data breach on or around April 13, 2015," they failed to notify customers or regulators of the data breach "until November 20, 2015 via [] internet press release." *Id.* ¶¶ 22–23. Within said press release, Starwood revealed "that hackers had breached its database containing sensitive records including: names, credit card numbers, security codes and expiration dates." *Id.* ¶ 2.

Plaintiff alleges that as a "member in the hotel chain's rewards program," he has frequented the spa at the Sheraton San Diego Hotel & Marina on a "continuous and ongoing basis." *Id.* ¶ 21. Plaintiff further alleges that during visits to the spa, "he provided personal identifying information and consumer information" to the hotel, operating under the "reasonable belief that [the information] would be held private." *Id.* Because of the approximately seven-month delay between discovering the data breach and notifying affected customers, Plaintiff alleges that hackers were given "months to use the information without the customers being able to take any steps to protect themselves." *Id.* ¶ 23.

The Sheraton San Diego Hotel & Marina was named as one of the hotels affected by the Starwood breach. *See id.* ¶ 24. As a customer of the hotel, Plaintiff alleges that his records "were among the records exposed." *Id.* Plaintiff alleges that during the time period between Starwood's initial discovery of the data breach and their disclosure that a breach had occurred, "[Plaintiff's] credit card . . . used for purchases at the Sheraton San Diego . . . was compromised by an unknown third party and used for unauthorized purchases, exposing him to losses, frustration and on-going requirements to protect himself from identity theft." *Id.* ¶ 26.

Plaintiff alleges that although "Starwood was fully aware of the consequences awaiting their customers if this information was accessed by third parties," "they failed to take even the basic precautionary measure of encrypting the data." *Id.* ¶ 28. As a result,

Plaintiff alleges that he and thousands of other Starwood customers have been "exposed . . . to violations of privacy, economic loss and risks of identity theft" for the rest of their lives. *Id.* ¶ 29.

PROCEDURAL BACKGROUND

On January 5, 2016, Plaintiff filed his First Amended Class Action Complaint alleging: (1) violation of the California Customer Records Act ("CRA"), Cal. Civ. Code §§ 1798.81.5, 1798.82; (2) violation of California's Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code §§ 17200, *et seq.*; (3) invasion of privacy; (4) negligence; and (5) negligence per se. FACC ¶¶ 39–84. Plaintiff has named Starwood Hotels & Resorts Worldwide, Inc., HST Lessee San Diego, LP and HST GP San Diego, LLC ("Defendants") as the collective defendants, alleging that Starwood is "the franchisor of the Sheraton brand," *id.* ¶ 14, while HST Lessee San Diego, LP and HST GP San Diego, LLC are concurrent "owner[s] or operator[s] of the Sheraton San Diego Hotel and Marina," *id.* ¶¶ 15–16. Plaintiff further alleges that each of the three defendants "ratified and approved" all the "actions of each defendant." *Id.* ¶ 19.

On February 26, 2016, Defendants moved to dismiss Plaintiff's Class Action Complaint. ECF No. 19. On March 18, 2016, Plaintiff filed his FACC. On April 1, 2016, Defendants filed a Motion to Dismiss Plaintiff's FACC ("Motion to Dismiss") based on (1) Plaintiff's failure to establish Article III standing and (2) Plaintiff's failure to state a claim on which relief can be granted. ECF No. 22. Plaintiff filed an opposition to Defendants' Motion to Dismiss on May 13, 2016. ECF No. 25. On June 3, 2016, Defendants filed a Reply to Plaintiff's Opposition. ECF No. 26.

DISCUSSION

I. STANDING TO SUE

A. Legal Standard

In order to invoke the subject matter jurisdiction of this Court, Plaintiff is required to establish standing to sue. Under Federal Rule of Civil Procedure ("Rule") 12(b)(1), a defendant may seek dismissal of a complaint for lack of subject matter jurisdiction. *See*

F.R.C.P. 12(b)(1). The federal court is one of limited jurisdiction. *See Gould v. Mut. Life Ins. Co. of N.Y.*, 790 F.2d 769, 774 (9th Cir. 1986). Each federal court has an "affirmative obligation to ensure that it is acting within the scope of its jurisdictional authority." *Grand Lodge of Fraternal Order of Police v. Ashcroft*, 185 F. Supp. 2d 9, 13 (D.D.C. 2001).

Plaintiff, as the party seeking to invoke jurisdiction, bears the burden of establishing jurisdiction. *See Kokkonen v. Guardian Life Ins. Co. of Am.*, 511 U.S. 375, 377 (1994). To meet this burden, Plaintiff must show:

> (1) that he or she has suffered an 'injury in fact' that is (a) "an invasion of a legally protected interest" that is concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) that the injury is fairly traceable to the challenged action of the defendant; and (3) that it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.

Lujan v. Defenders of Wildlife, 504 U.S. 555, 559–60 (1992) (internal citations omitted). Because these elements are "not mere pleading requirements but rather an indispensable part of the plaintiff's case," Plaintiff bears the burden of proving — "with the manner and degree of evidence required at the successive stages of litigation" — that he has Article III standing. *See id.* at 561. At the pleading stage, general factual allegations of injury are sufficient for standing purposes because courts, on a motion to dismiss, will "presum[e] that general allegations embrace those specific facts that are necessary to support the claim." *See Lujan v. Defenders of Wildlife*, 497 U.S. 871, 889 (1990).

With regard to injury in fact, a plaintiff must show that he suffered "an invasion of a legally protected interest" that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical." *Lujan*, 504 U.S. at 560 (internal citations omitted). A "concrete" injury must be "*de facto*," meaning, it must actually exist. *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016). The "threatened injury must be *certainly impending* to constitute injury in fact" and "allegations of *possible* future injury are not sufficient." *Clapper v. Amnesty Intern. USA*, 133 S. Ct. 1138, 1147 (emphasis in original) (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990)). In *Clapper*, the

Supreme Court held that respondents' reliance on a "highly attenuated chain of possibilities," involving a "highly speculative fear" that a number of third party actors would take certain actions, did not amount to the "certainly impending" injury required for Article III standing. *Clapper*, 133 S. Ct. at 1148.

To prove "causation," a plaintiff must show that the injury is fairly traceable to the challenged action of the defendant, and that the injury is not the result of the independent action of a third party not before the court. *Lujan*, 504 U.S. at 560.

The third and final element of standing, redressability, does not appear in the text of the Constitution. Rather, it is a judicial creation of the past twenty-five years and an interpretation of the "case" requirement of Article III standing. *See Simon v. Eastern Ky. Welfare Rights Org.*, 426 U.S. 26, 38, 41–46 (1976). To demonstrate redressability, a plaintiff must show that the injury "is likely to be redressed by a favorable decision." *Id.* at 38, 41. Consequently, the Supreme Court has found that "psychic satisfaction is not an acceptable Article III remedy because it does not redress a cognizable Article III injury." *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 107 (1998) (explaining that because respondent sought "vindication of the rule of law" rather than "remediation of its own injury" it had not established redressability because "[r]elief that does not remedy the injury suffered cannot bootstrap a plaintiff into federal court; that is the very essence of the redressability requirement").

B. Injury in Fact

Injury-in-fact analysis is highly case-specific. This is particularly true in the context of data breach. To determine whether or not a plaintiff was, in fact, injured by a defendant's data breach, various courts have found one or more of following factors persuasive: (1) the type and volume of stolen information[1]; (2) the likelihood that the

[1] *See Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1141–43 (9th Cir. 2010) (holding that theft of plaintiffs' names, addresses, and social security numbers amounted to injury in fact because acquisition of that information exposed plaintiffs to an increased risk of future identity theft, which was a "credible threat of real and immediate harm").

information was stolen for misuse[2]; (3) the degree of attenuation between the theft and the harm[3]; (4) whether the stolen information has been misused[4]; and (5) whether unauthorized purchases were reimbursed[5].

Defendant argues that the gravamen of Plaintiff's allegations amounts to nothing more than a "fear[ ] of hypothetical future harm," *see Clapper*, 133 S. Ct. at 1151, that could be inflicted by future unauthorized expenditures. A plaintiff, however, cannot manufacture standing by causing harm to oneself based on "hypothetical future harm that is certainly not impending." *Id.*; *see also In re Adobe Systems, Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1216 (N.D. Cal. 2014). In *Clapper*, the respondents' "feared" that: "(1) the Government will decide to target the communications of non-U.S. persons with whom they communicate; (2) in doing so, the Government will choose to invoke its authority under [Section 702] rather than utilizing another method of surveillance; (3) the Article III judges who serve on the Foreign Intelligence Surveillance Court will conclude

---

[2] *See In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1214–15 (N.D. Cal. 2014) (concluding that likelihood that plaintiff's personal information would be misused was "certainly impending" given that third-parties had targeted defendants' servers, spent weeks collecting personal information, had decrypted credit card numbers, and given that some stolen information had surfaced on the Internet).

[3] *See Reilly v. Ceridian Corp.*, 664 F.3d 38, 42 (3rd Cir. 2011) (finding that plaintiffs lacked standing because their allegations of harm were hypothetical and relied on speculation that the hacker read, copied, and understood their personal information; that they intended to use the information to commit future criminal acts; and that they had the capacity to make unauthorized transactions in the future).

[4] *See Key v. DSW, Inc.*, 454 F. Supp. 2d 684, 689–90 (S.D. Ohio 2006) (concluding that no injury in fact occurred when plaintiff had alleged that unauthorized persons had obtained access to personal customer information because the allegations amounted only to the "possibility of harm at a future date"); *see also Hinton v. Heartland Payment Sys., Inc.*, 2009 WL 704139, at *1 (D.N.J. Mar. 16, 2009) (sua sponte dismissing case because plaintiff failed to assert that a third party has actually used his credit information to either open a credit card account or otherwise secure a fraudulent benefit and because allegations of increased risk of identity theft and fraud "amount[ed] to nothing more than mere speculation"); *Bell v. Acxiom Corp.*, 2006 WL 2850042, at *2 (E.D. Ark. Oct. 3, 2006) (rejecting plaintiff's allegation of increased risk of identity theft where plaintiff had not alleged that she had suffered anything greater than an increased risk of identity theft).

[5] *See Whalen v. Michael Stores Inc.*, 153 F. Supp. 2d 577, 580–81 (E.D.N.Y. 2015) *appeal docketed*, No. 16-352 (2d Cir. Feb. 5, 2016) (finding failure to allege injury in fact because, among other things, plaintiff had failed to allege that she suffered an unreimbursed charge); *see also Hammond v. Bank of New York Mellon Corp.*, 2010 WL 2643307, at *8 (S.D.N.Y. June 25, 2010) (Article III standing lacking where unauthorized charges from misuse of personal information were reimbursed).

that the Government's proposed surveillance procedures satisfy [Section 702's] many safeguards and are consistent with the Fourth Amendment; (4) the Government will succeed in intercepting the communications of respondents' contacts; and (5) respondents will be parties to the particular communications that the Government intercepts." 133 S. Ct. at 1148. Given the level of attenuation between this feared action and the likelihood of harm, the court concluded that the future harm was too hypothetical to qualify as injury in fact. Meanwhile, the instant case involves more than unrealized or hypothetical actions by third parties. Here, Plaintiff's name and credit card information have been stolen and an unauthorized individual has already made charges on Plaintiff's credit card. Thus, the question before the Court is whether the theft of Plaintiff's personal identifying information ("PII") and the subsequent unauthorized purchases sufficiently establish a "concrete and particularized" harm that is "actual or imminent, not conjectural or hypothetical."

Plaintiff claims various forms of harm individually and on behalf of the class members. They include:

> (1) theft of their names and credit card information; (2) costs associated with the detection and prevention of identity theft or unauthorized use of financial accounts and credit card records; (3) lost opportunity costs and loss of productivity from efforts to mitigate the actual and future consequences of the data theft, including fraudulent charges, cancelling and reissuing credit cards, purchasing credit monitoring and identity theft protection, and the stress of dealing with all issues resulting from the data theft; (4) cost associated with the inability to use credit; (5) future costs in terms of time, effort, and money that will be expended to prevent and repair the impact of the data breach; (6) damages to and diminution in value of information entrusted to Defendants for the purpose of deriving health care from Defendants[6]; (7) the imminent and certainly impending injury flowing from potential fraud and identity theft posed by the data breach; and (8) the continued risk to their credit card information, which is subject to further breaches so long as Defendants fail to undertake adequate measures to protect data in their possession.

---

[6] Plaintiff has alleged this form of harm even though it is confined to cases involving medical information under Cal. Civ. Code § 56.10 *et seq.* While Plaintiff references this section in identifying common issues of fact, there are no allegations that Defendants are health care providers and that § 56.10 applies to them. FACC ¶¶ 38, 70.

FACC ¶¶ 56, 70, 74.

These claimed injuries can be summarized as (1) past financial costs associated with detecting and preventing identity theft or unauthorized use of credit cards; (2) future costs in terms of time, effort and money to prevent or repair identity theft or future unauthorized use of credit cards; (3) theft of personal identifying information and; (4) past loss of productivity from efforts to mitigate consequences of data theft.

1. Past Financial Costs

As to past financial costs, other than conclusory allegations, Plaintiff has not specifically alleged out-of-pocket losses or monetary damages resulting from the data breach due to Defendants' negligence or "failure to maintain reasonable security procedures." *See generally* Cal. Civ. Code § 1798.81.5(b).[7] As to fraudulent charges, Plaintiff does not assert that he suffered any unreimbursed losses from the unauthorized use of his credit card or that he was unable to use credit thereafter. Plaintiff merely alleges that he was "exposed" to economic losses. *Id*. ¶¶ 26, 29. Such indirect allegations do not demonstrate injury in fact. The FACC instead offers only oblique references to "unauthorized purchases" and "damages" suffered by Plaintiff and the putative class. *See, e.g.*, FACC ¶¶ 1, 12, 26. But these "conclusory allegations" and "general averments" are inadequate to establish standing. *See Friends of the Earth, Inc. v. Laidlaw Envtl. Servs., Inc.*, 528 U.S. 167, 184 (2000) (citations omitted).

2. Future Harm

With respect to future damages and mitigating future loss in data theft cases, the Ninth Circuit has identified the types of data breaches which constitute a "real and immediate harm" as opposed to a merely "conjectural or hypothetical" harm. *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010). In *Krottner*, Plaintiffs were Starbucks employees whose personal information, including names, addresses, and social

[7] In his FACC, Plaintiff only seeks injunctive relief, declaratory relief, and attorney fees, and only reserves a right to seek damages. FACC ¶¶ 45, 64, 72, 84.

security numbers were compromised as a result of the theft of a company laptop. *Id.* at 1140. The Ninth Circuit found that the *Krottner* plaintiffs satisfied the injury-in-fact requirement because they had "alleged a credible threat [of future identity theft] of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data." *Id.* at 1143. Thus, where sensitive personal data, such as names, addresses, social security numbers, and credit card numbers are improperly disclosed or disseminated into the public — thereby increasing the risk of future harm to plaintiff — injury in fact has been sufficiently alleged. *Id.* at 1139; *Doe 1 v. AOL*, 719 F. Supp. 2d 1102, 1109–11 (N.D. Cal. 2010).

A similar conclusion was reached in *In re Adobe*, 66 F. Supp. 3d at 1214, where plaintiffs alleged that "hackers deliberately targeted Adobe's servers and spent several weeks collecting names, usernames, passwords, emails addresses, phone numbers, mailing addresses, credit card numbers and expiration dates." The *Adobe* court concluded that the risk that the plaintiffs' personal data would be misused by the hackers was "immediate and very real" because it was clear that the hackers "intend[ed] to misuse the personal information stolen" and that they had the ability to do so. *Id.* at 1214–15. Accordingly, the court concluded that Article III standing to bring a CRA claim for violations of Section 1798.81.5 did exist because plaintiff had adequately alleged injury in fact, causation, and redressability. *Id.* at 1217.

Here, the theft of personal information is far more limited than that in *Krottner* and *In re Adobe*, and notably, does not involve the theft of social security information or the theft of usernames, passwords, or emails. Plaintiff only alleges that the Starwood breach jeopardized the names, addresses, billing information, and credit card numbers of the members of the hotel's chain rewards program. FACC ¶ 2. This fact is salient with respect to future identity theft because the information stolen during the Starwood breach is insufficient, for example, for a third party to open up a new account in Plaintiff's name or to gain access to personal accounts likely to have the information needed to open such an account (e.g., a social security number). Thus, in order for the Court to conclude that

there is any credible, future risk of identity theft it would have to speculate as to whether a third-party with only Plaintiff's name and address could engage in wholesale identity theft. What's more, as is made clear by Plaintiff's request to be compensated for the time and money he lost in the process of cancelling his compromised credit card, *see* FACC ¶¶ 70, 71, 82, the theft of Plaintiff's credit card poses no future threat of identity theft as it is no longer active. Thus, unlike in *In re Adobe* where it was clear that the third-party had the ability to engage in future identify theft, here, the Court would have to engage in a hypothetical line of reasoning in order to conclude that Plaintiff remains at risk of imminent identity theft given the small amount of useful personal information that a third-party potentially has at its fingertips. *See Antman v. Uber Techs., Inc.*, 2015 WL 6123054, *11 (N.D. Cal. Oct. 19, 2015) (concluding that theft of plaintiff's name and driver's license was insufficient to demonstrate injury in fact because any harm that would result from such a misappropriation posed no credible risk of identity theft). Accordingly, because the PII stolen was limited only to Plaintiff's name, address, and credit card information, and because the credit card has since been cancelled, the Court finds that Plaintiff has not sufficiently alleged the credible threat of future identity theft needed in order to plead injury in fact for his causes of action.

3. Theft of PII

Plaintiff alleges that he incurred a recognizable loss by the theft of his personal identifying information. In so doing, Plaintiff claims a property right to personal identifying information, but fails to identify any authority to support this proposition. Without more, the Court finds that the claimed loss of PII does not constitute a concrete harm sufficient for standing purposes. *Cf. Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 968 (7th Cir. 2016) (refusing to recognize a property right to personally identifiable data as a basis for standing to sue in a data breach case). Nor does the mere violation of a consumer protection statute establish a "concrete" injury. *See Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549–50 (2016) ("Congress' role in identifying and elevating intangible harms does not mean that a plaintiff automatically satisfies the injury-in-fact

requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right."). Thus, the Court concludes that alleging theft of PII, without more, is inadequate to demonstrate a harm that qualifies as an injury in fact for standing purposes.

4. Past Anxiety and Loss of Time to Mitigate or Avoid Harm

In this case, the FACC alleges lost time and expenses associated with "mitigat[ing] the actual . . . consequences of the data theft." FACC ¶¶ 70, 82. Defendants, in turn, argue that the FACC does not allege any facts demonstrating that Plaintiff suffered such lost time and expense. Plaintiff, however, has indicated that the alleged source of the injury is the stress and costs associated with "cancelling and reissuing credit cards," *id.* ¶ 70, and the "loss of productivity from efforts to mitigate the actual and future consequences of the theft of their identifying information and credit card records," *id.* ¶ 56.

The Supreme Court has observed that "concrete" for purposes of standing is not necessarily synonymous with "tangible." *Spokeo, Inc.*, 136 S. Ct. at 1549 ("Although tangible injuries are perhaps easier to recognize . . . intangible injuries can nevertheless be concrete.") Although the Ninth Circuit has not yet decided whether anxiety or lost time to avoid financial loss qualifies as concrete injury, the Seventh Circuit has held that the loss of time resulting from a plaintiff taking action to mitigate the misuse of a credit card constitutes injury in fact. In *Remijas v. Neiman Marcus Grp., LLC*, the Seventh Circuit concluded that the time and money class members spent on resolving fraudulent charges and protecting against future identity theft was sufficient for standing purposes, even if the bank ultimately repaid the charges, because the customers "suffered the aggravation and loss of value of the time needed to set things straight, to reset payment associations after credit card numbers are changed, and to pursue relief for unauthorized charges." 794 F.3d 688, 693–94 (7th Cir. 2015); *accord Lewert*, 819 F.3d at 967. Likewise, other district courts in the Ninth Circuit have ruled similarly. Recently, Judge Lucy Koh, relying on *Lewert* and *Remijas*, extended her ruling in *In re Adobe* to conclude

that a Plaintiff's "us[e] [of] their own time for credit monitoring" in response to a data breach was a recoverable harm. *See In re Anthem, Inc. Data Breach Litig.*, 2016 WL 3029783, at *26 (N.D. Cal. May 27, 2016).

Here, Plaintiff has alleged that his credit card information was stolen and misused and that he arranged to cancel and reissue the compromised credit card after learning that his PII was misused. He further alleges that the need to mitigate his exposure to fraudulent charges and potential identity theft resulted in a loss of productivity. These allegations present a concrete, non-speculative harm that befell Plaintiff as a result of the Starwood breach. Accordingly, to the extent Plaintiff seeks relief for the loss of time and money spent to avoid losses caused by the data breach, his allegations are sufficient to state an injury in fact.

C. Causation

With regards to Plaintiff's claim arising under Section § 1798 of the California Customer Records Act, FACC ¶¶ 39–47, Defendants argue that the FACC asserts no factual basis for the conclusion that Defendants' alleged delayed in notifying Starwood customers of the data breach caused any harm. The Court agrees.

Section 1798.82 of the CRA requires businesses to "disclose a breach of the security of the system following discovery or notification of the breach . . . in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82(a). While Plaintiff alleges that Defendants' "failure to provide prompt notice contributed to his losses," Plaintiff does not provide any further factual support demonstrating that Defendants' alleged violation of Section 1798.82 resulted in a cognizable injury in fact to himself or other class members. *See* ECF No. 25 at 6–7. Reviewing the FACC and Plaintiff's Opposition to Defendant's Motion to Dismiss, it is entirely unclear how any of the injuries identified by Plaintiff have been caused or compounded by Defendants' alleged failure to promptly notify Plaintiff or other class members of the Starwood breach. Plaintiff also does not allege any incremental harm suffered as a result of the

/ / / /

alleged delay in notification. As such, Plaintiff has failed to allege any harm resulting from Defendants' purported delay in notifying Starwood customers of the breach.

This conclusion, moreover, comports with the court's decision in *In re Adobe*, where it concluded that plaintiffs had failed to plausibly allege that Adobe's delay in notifying customers of a 2013 data breach resulted in injury. 66 F. Supp. 3d at 1218 ("Plaintiffs have not alleged any injury traceable to Adobe's alleged failure to notify customers of the 2013 data breach in violation of Section 1798.82, because [p]laintiffs do not allege that they suffered any incremental harm as a result of the delay"). Just as the *In re Adobe* court concluded that Plaintiff had failed to allege injury in fact because Plaintiff had not traced any injury from the delayed notification, the Court, here, concludes that Plaintiff has not alleged injury in fact because he does not indicate what, if any, concrete harm resulted from Defendants' alleged failure to promptly notify Starwood customers of the data breach. Accordingly, because Plaintiff has failed to trace any harm from Defendants' delayed notification or to demonstrate a nexus between the alleged harm flowing from the delayed notification and Defendants' actions, Plaintiff has failed to adequately alleged causation with respect to his CRA § 1798.82 claim.

Defendants further argue that Plaintiff has also failed to sufficiently allege that Defendants' failure to maintain reasonable security practices, or Defendants' alleged violation of Section 1798.81.5(b) of the CRA, caused Plaintiff any injury in fact. Defendants point out that the FACC does not allege that the Starwood breach — as opposed to another contemporaneous data breach or other possible source of fraud — actually caused the unspecified fraudulent charges that Plaintiff allegedly suffered on his credit card. Yet the fact that other data breaches might have caused Plaintiff's private information to be exposed does nothing to negate Plaintiff's standing to sue here, given that Plaintiff has made a plausible showing, sufficient for pleading purposes, to demonstrate that his injuries are "fairly traceable" to the Starwood breach. *See Neiman Marcus*, 794 F.3d 688, 693–94 (7th Cir. 2015); *see also In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1159 (D. Minn. 2014) ("Plaintiffs' allegations

plausibly allege that they suffered injuries that are 'fairly traceable' to Target's conduct. This is sufficient at this stage to plead standing. Should discovery fail to bear out Plaintiffs' allegations, Target may move for summary judgment on the issue.") (citations omitted); *Lewert*, 819 F.3d at 969 (stating that "[m]erely identifying potential alternative causes does not defeat standing").

The Court, therefore, finds that Plaintiff has insufficiently alleged causation for standing purposes as to his § 1798.82 claim and sufficiently alleged it as to his § 1798.81.5, UCL, right of privacy, and negligence claims.

D. Redressability

To demonstrate redressability, a plaintiff must show that the injury "is likely to be redressed by a favorable decision." *Simon v. Eastern Ky. Welfare Rights Org.*, 426 U.S. 26, 38, 41 (1976). In the context of a class action suit, plaintiffs must also "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, 503 (1975). Consequently, "if 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 [herself] or any other member of the class." *O'Shea v. Littleton*, 414 U.S. 488, 494 (1974) (citations omitted); *see also Bailey v. Patterson*, 369 U.S. 31, 32–33 (1962); *Indiana Emp't Sec. Div. v. Burney*, 409 U.S. 540, 544–45 (1973).

1. Damages

A plaintiff's injuries cannot be redressed by a judicial decision to the extent that they have already been reimbursed for fraudulent charges. However, while this may be true for the fraudulent charges, it is not necessarily true for the mitigation expenses or the future injuries. *Remijas*, 794 F.3d at 697; *Lewert*, 819 F.3d at 969 (in establishing redressability, all class members should have the chance to show that they spent time and resources tracking down the possible fraud, changing automatic charges, and replacing cards as a prophylactic measure).

Here, the Court has concluded that Plaintiff's allegations that he lost time and money in the process of mitigating financial losses caused by the Starwood breach are sufficient to state an injury in fact. Because Plaintiff has not been reimbursed in any way for that expenditure of time and money, the Court concludes that the injury is redressible by judicial decision and, thus, is sufficient to allege the final element of Article III standing as to Plaintiff's request for damages.

2. Injunctive Relief

Plaintiff must demonstrate standing for each form of relief he seeks. *See Friends of the Earth, Inc.*, 528 U.S. at 185. Plaintiff, thus, bears the burden of showing that he "personally would benefit in a tangible way" from the prospective injunctive and declaratory relief he requests. *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 103 n.5 (1998). Furthermore, where a named plaintiff seeks injunctive relief, the plaintiff must demonstrate that he or she — and any other proposed class members — are "realistically threatened by a repetition of the violation." *Gest v. Bradbury*, 443 F.3d 1177, 1181 (9th Cir. 2006) (citing *Armstrong v. Davis*, 275 F.3d 849, 860–61 (9th Cir. 2001)); *see also City of Los Angeles v. Lyons*, 461 U.S. 95, 109 (1983) ("If Lyons has made no showing that he is realistically threatened by a repetition of his experience . . . he has not met the requirements for seeking an injunction in a federal court."); *DeFunis v. Odegaard*, 416 U.S. 312, 319 (1974) (explaining that the named plaintiff must make a reasonable showing that he will again be subjected to the alleged illegality).

In the instant case, Plaintiff fails to establish "redressability" as to the request for injunctive relief because Plaintiff does not sufficiently allege that he is "realistically threated by a repetition of his experience" that is "likely to be redressed by a favorable decision" by this Court. *Simon*, 426 U.S. at 38, 41. Plaintiff contends that the relief he seeks via an injunction is obtainable because of his "fear of on-going data breaches" and "inten[t] to continue as a customer if his data can be adequately protected." ECF No. 25 at 4. However, as Defendants point out, "an order requiring Defendants to enhance their cybersecurity in the future (or an equivalent declaratory judgment) will not provide any

relief for past injuries or injuries incurred in the future because of a data breach that has already occurred." ECF No. 22 at 12. The Court agrees with Defendants in this regard. If the Court were to issue injunctive relief based on Defendants' alleged past violations of § 1798.81.5(b) and § 1798.82 of the CRA, the relief afforded would be mostly "psychic satisfaction." *See Steel Co.*, 523 U.S. at 107 ("psychic satisfaction is not an acceptable Article III remedy because it does not redress a cognizable Article III injury"). Accordingly, the Court concludes that Plaintiff has failed to establish redressability as to his request for injunctive relief.

To conclude: in view of the foregoing analysis of the standing factors, the Court **GRANTS** Defendants' Rule 12(b)(1) motion to dismiss as to Plaintiff's § 1798.82 CRA claim and Plaintiff's request for injunctive relief and **DENIES** Defendants' 12(b)(1) motion to dismiss as to Plaintiff's § 1798.81.5, UCL, negligence, and invasion of privacy causes of action.

II. FAILURE TO STATE A CLAIM

A. Legal Standard

A motion to dismiss under Rule 12(b)(6) tests the sufficiency of a complaint. *Navarro v. Block*, 250 F.3d 729, 732 (9th Cir. 2001). Dismissal is warranted where the complaint lacks a cognizable legal theory. *Robertson v. Dean Witter Reynolds, Inc.*, 749 F.2d 530, 534 (9th Cir. 1984); *see Neitzke v. Williams*, 490 U.S. 319, 326 (1989) ("Rule 12(b)(6) authorizes a court to dismiss a claim on the basis of a dispositive issue of law."). Alternatively, a complaint may be dismissed where it presents a cognizable legal theory yet fails to plead essential facts under that theory. *Robertson*, 749 F.2d at 534. While a plaintiff need not give "detailed factual allegations," a plaintiff must plead sufficient facts that, if true, "raise a right to relief above the speculative level." *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 545 (2007).

"To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Twombly*, 550 U.S. at 547). A claim is

facially plausible when the factual allegations permit "the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* In other words, "the non-conclusory 'factual content,' and reasonable inferences from that content, must be plausibly suggestive of a claim entitling the plaintiff to relief." *Moss v. U.S. Secret Serv.*, 572 F.3d 962, 969 (9th Cir. 2009).

"Determining whether a complaint states a plausible claim for relief will . . . be a context-specific task that requires the reviewing court to draw on its judicial experience and common sense." *Iqbal*, 556 U.S. at 679. In reviewing a motion to dismiss under Rule 12(b)(6), a court must assume the truth of all factual allegations and must construe all inferences from them in the light most favorable to the nonmoving party. *Thompson v. Davis*, 295 F.3d 890, 895 (9th Cir. 2002); *Cahill v. Liberty Mut. Ins. Co.*, 80 F.3d 336, 337–38 (9th Cir. 1996). Legal conclusions, on the other hand, need not be taken as true merely because they are cast in the form of factual allegations. *Ileto v. Glock, Inc.*, 349 F.3d 1191, 1200 (9th Cir. 2003); *Western Mining Council v. Watt*, 643 F.2d 618, 624 (9th Cir. 1981). When ruling on a motion to dismiss, a court may consider the facts alleged in the complaint, documents attached to the complaint, documents relied upon but not attached to the complaint when authenticity is not contested, and matters of which the court takes judicial notice. *Lee v. City of Los Angeles*, 250 F.3d 668, 688–89 (9th Cir. 2001).

Where a motion to dismiss is granted, "leave to amend should be granted 'unless the court determines that the allegation of other facts consistent with the challenged pleading could not possibly cure the deficiency.'" *DeSoto v. Yellow Freight Sys., Inc.*, 957 F.2d 655, 658 (9th Cir. 1992) (quoting *Schreiber Distrib. Co. v. Serv-Well Furniture Co.*, 806 F.2d 1393, 1401 (9th Cir. 1986)). In other words, where leave to amend would be futile, a court may deny leave to amend. *See DeSoto*, 957 F.2d at 658.

A holding that a plaintiff has pled an injury in fact for purposes of Article III standing does not establish that he adequately pled his cause of action. *See Doe v. Chao*,

540 U.S. 614, 624–25 (2004) (explaining that an individual may suffer Article III injury and yet fail to plead a proper cause of action.)

B. Analysis

1. California Customer Records Act

CRA Section 1798.81.5(b) states:

> 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.

Cal. Civ. Code § 1798.81.5(b). CRA Section 1798.82, in relevant part, states:

> A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement . . . or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Id. § 1798.82(a).

Plaintiff alleges that Defendants violated the California CRA in two ways: (1) by failing to "implement and maintain reasonable security procedures," *see* FACC ¶ 43, and (2) by failing to notify affected customers in a timely manner, *see id.* ¶ 44.

As an initial matter, proof of damages is a threshold hurdle for both CRA causes of action. *See* Cal. Civ. Code § 1798.84(b) (permitting suit by "[a]ny customer *injured by* a violation of [the CRA]") (emphasis added). As concluded above, Plaintiff has failed to allege any injury proximately caused by any violation of § 1798.82(a). Accordingly, Plaintiff has failed to state a cause of action under § 1798.82. Thus, only Plaintiff's § 1798.81.5 claim remains. However, that Plaintiff has pled an injury in fact for purposes of Article III standing as to the § 1798.81.5 claim does not establish that he has adequately pled damages for the cause of action. *See Doe v. Chao*, 540 U.S. at 624–25.

Plaintiff, therefore, must have sufficiently alleged that he was *injured by* a violation of the CRA in order for the cause of action to survive the motion to dismiss.[8]

Defendants argue that Plaintiff has failed to allege sufficient facts demonstrating that Defendants failed to maintain reasonable cybersecurity practices as required by § 1798.81.5. ECF 22-1 at 23. More specifically, Defendants assert that the FACC, primarily, only offers legal conclusions and hyperbole in support of the claim. *See, e.g.*, FACC ¶ 6 ("Instead of installing proper safeguards, Starwood essentially invited the information to be stolen, exposing highly valuable and private information of its customers."). While it is true that Plaintiff's FACC is short on specifics, one allegation that does gives some indication of how Defendants' cybersecurity was supposedly insufficient states that "Starwood, among other things, failed to 'appropriately encrypt customers' data in its possession." *Id.* ¶¶ 6, 28. Plaintiff separately suggests that Defendants' "security systems and protocols" should have been designed, implemented, maintained, and tested "consistent with industry standards and requirements." *Id.* ¶ 66.

The Court finds that Plaintiff has sufficiently alleged, at the pleading stage, a legal duty and a corresponding breach as to inadequate security measures. *See In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 966 (S.D. Cal. 2014) (holding that plaintiffs had adequately alleged breach of duty to provide reasonable security by pleading that they gave personal information to Sony as part of commercial transaction, and that Sony failed to employ reasonable security measures to protect the information, including failing to use industry-standard encryption); *see also Witriol v. LexisNexis Grp.*, 2006 WL 4725713, at *7–8 (N.D. Cal. Feb. 10, 2006) (denying defendants' motion to dismiss negligence claim based on failure to protect security and confidentiality of consumer information because plaintiff had sufficiently

[8] Neither party has addressed whether "injury" under § 1798.84(b) extends to non-monetary forms of loss. Without further briefing on this question, the Court will not sua sponte address the issue or rely on it in considering the motion to dismiss.

alleged a corresponding duty owed to plaintiffs). Because Plaintiff alleges that he provided his PII to Defendants as part of a commercial transaction, and that Defendants failed to employ reasonable security measures to protect such PII, such as the utilization of industry-standard encryption, the Court finds that Plaintiff has sufficiently alleged a legal duty and a corresponding breach at this stage.

For the foregoing reasons, the Court finds that Plaintiff has plausibly alleged a cause of action based upon the lack of reasonable security procedures under § 1798.81.5, and failed to allege a cause of action for failure to notify customers in a timely fashion under § 1798.82(a). Thus, the Court **GRANTS** Defendants' motion to dismiss the § 1798.82(a) claim without prejudice and **DENIES** Defendant's motion to dismiss the § 1798.81.5 claim.

2. California Unfair Competition Law

California's Unfair Competition Law ("UCL") provides a cause of action for business practices that are (1) unlawful, (2) unfair, or (3) fraudulent. Cal. Bus. & Prof. Code § 17200, *et seq*. Plaintiff alleges that Defendants' acts and practices violating § 1798.90, *et seq*., of the CRA constitute unlawful and unfair business practices. *See generally* FACC ¶¶ 48–55.

In order for Plaintiff to sue Defendants for unlawful and unfair business practices, Plaintiff must also demonstrate that it has UCL-specific standing. In order to establish standing under the UCL, a plaintiff's claim must specifically involve lost money or property. *See Kwikset Corp. v. Superior Court*, 246 P.3d 877, 886 (Cal. 2011); *Troyk v. Farmers Group, Inc.*, 171 Cal. App. 4th 1305, 1348 n.31 (Cal. Ct. App. 2009) ("[The] UCL's standing requirements appear to be more stringent than the federal standing requirements. . . . Proposition 64 . . . added a requirement that a UCL plaintiff's 'injury in fact' specifically involve 'lost money or property.' (Cal. Bus. & Prof. Code, § 17204)"); *Ehret v. Uber Techs., Inc.*, 68 F. Supp. 3d 1121, 1132 (N.D. Cal. 2014) ("Whereas a

/ / / /

/ / / /

federal plaintiff's injury in fact may be intangible and need not involve lost money or property, . . . a UCL plaintiff's injury in fact [must] specifically involve lost money or property.") (internal quotation marks omitted).

Here, Plaintiff has alleged that unauthorized charges were made on his credit card, that he will incur damages to monitor identity theft, and that he has spent time responding to the unauthorized charges on his credit card. As discussed above in the Standing section, none of these allegations demonstrate that Plaintiff has suffered a loss of money or property. In addition, as stated above, Plaintiff has, moreover, failed to establish that the loss of his PII constitutes a form of property that could qualify as property under the UCL.

Thus, the Court **GRANTS** Defendant's motion to dismiss Plaintiff's second cause of action for violation of California's UCL without prejudice.

3. Invasion of Privacy

Under California law, to adequately state a claim for invasion of privacy, a plaintiff must demonstrate three elements: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy under the circumstances; and (3) a serious invasion of the privacy interest. *See, e.g., Hill v. Nat'l Collegiate Athletic Ass'n*, 865 P.2d 633, 654–55 (Cal. 1994).

Plaintiff's FACC does not allege sufficient facts to plead an invasion of a legally protected privacy interest, *see generally* FACC ¶¶ 58–64, and Plaintiff's legal conclusions that "Defendants are guilty of oppression, fraud, or malice by permitting unauthorized disclosure of Plaintiff's [] personal credit card information with a willful and conscious disregard of Plaintiff's [] right to privacy" do not sufficiently demonstrate a "serious invasion of privacy," *see id.* ¶ 63. Plaintiff fails, for example, to allege any facts that would suggest that the data breach was an intentional violation of Plaintiff's and other class members' privacy, as opposed to merely a negligent one. *See In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) (citing *Ruiz v. Gap, Inc.*, 540 F. Supp. 2d 1121, 1127–28 (N.D. Cal. 2008), *aff'd*, 380 F. App'x 689 (9th

Cir. 2010) (stating that "[e]ven negligent conduct that leads to theft of highly personal information, including social security numbers, does not 'approach [the] standard' of actionable conduct under the California Constitution and thus does not constitute a violation of Plaintiffs' right to privacy").

Thus, the Court **GRANTS** Defendant's motion to dismiss Plaintiff's third cause of action for invasion of privacy without prejudice.

4. Negligence

Plaintiff alleges that Defendants did not "take adequate security measures to protect the information they obtained," FACC ¶ 21; *see also* ECF No. 25 at 7, and that Defendants owed a duty to Plaintiff and class members "to exercise reasonable care in . . . securing, safeguarding, and protecting . . . personal information," FACC ¶ 66, and to "timely disclose any incidents of data breaches," *id.* ¶ 68. As a result of Defendants' alleged breach of these duties, Plaintiff alleges numerous injuries suffered by Plaintiff and class members, including theft of their credit card information, costs associated with prevention of identity theft, and costs associated with time spent and loss of productivity, among other injuries. *See id.* ¶ 70.

Generally speaking, in actions for negligence, liability is limited to damages for physical injuries and recovery of economic loss is not allowed. *See Aas v. Superior Court of San Diego Cty.*, 24 Cal. 4th 627, 636 (Cal. 2000) (citing *Seely v. White Motor Co.*, 63 Cal. 2d 9, 23 (Cal. 1965)); *cf. Krottner v. Starbucks Corp.*, 406 F. App'x 129, 131 (9th Cir. 2010) (no cognizable injury on negligence claim where no loss related to an attempt to open a bank account was alleged and plaintiff waived any argument that his alleged anxiety constituted an actionable injury). In the absence of (1) personal injury, (2) physical damage to property, (3) a special relationship existing between the parties, or (4) some other common law exception to the rule, recovery of purely economic loss is foreclosed. *See Kalitta Air, LLC v. Cent Tex. Airborne Sys., Inc.*, 315 F. App'x 603, 605 (9th Cir. 2008) (quoting *J'Aire Corp. v. Gregory*, 598 P.2d 60, 63–65 (Cal. 1979)). Here, Plaintiff alleges nothing more than pure economic loss. Plaintiff alleges no personal

injury or physical damage to his property, and puts forth no facts to demonstrate that a special relationship existed between him and Defendants. *See* FACC ¶ 29.

Thus, the Court **GRANTS** Defendant's motion to dismiss Plaintiff's fourth cause of action for negligence without prejudice.

5. Negligence Per Se

In California, negligence per se is "a presumption of negligence [that] arises from the violation of a statute which was enacted to protect a class of persons of which the plaintiff is a member against the type of harm which the plaintiff suffered as a result of the violation of the statute." *See, e.g.*, *Hoff v. Vacaville Unified Sch. Dist*., 19 Cal. 4th 925, 938 (Cal. 1998) (citations omitted). Accordingly, negligence per se is simply a codified evidentiary doctrine and does not per se establish tort liability. *Quiroz v. Seventh Ave. Ctr*., 140 Cal. App. 4th 1256, 1284–85 (Cal. Ct. App. 2006). Stated differently, negligence per se does not state an independent cause of action because "[t]he doctrine does not provide a private right of action for violation of a statute." *People of California v. Kinder Morgan Energy Partners, L.P*., 569 F. Supp. 2d 1073, 1087 (S.D. Cal. 2008) (quoting *Quiroz*, 140 Cal. App. 4th at 1285.)

Thus, the Court **GRANTS** Defendant's motion to dismiss Plaintiff's fifth cause of action for negligence per se with prejudice.

CONCLUSION

For the foregoing reasons, **IT IS HEREBY ORDERED** that:

1. Defendants' Motion to Dismiss, (ECF. No. 22), be **GRANTED** in part and **DENIED** in part.
2. Federal Rule of Civil Procedure 15 provides that courts should freely grant leave to amend "when justice so requires." Accordingly, the Court **GRANTS** Plaintiff **twenty (20) days** from the issuance of this Order to file a Second Amended Complaint that addresses the pleading deficiencies noted above. Failure to meet the twenty-day deadline to file an amended complaint or failure to cure the deficiencies identified in this Order will result in a dismissal with

prejudice. Plaintiffs may not add new causes of actions or parties without leave of the Court or stipulation of the parties pursuant to Rule 15.

IT IS SO ORDERED.

Dated: November 3, 2016

Hon. Gonzalo P. Curiel
United States District Judge