UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES - GENERAL

Case No.	**14-CV-09600 RGK (Ex)**	Date	June 15, 2015
Title	***MICHAEL CORONA, et al v. SONY PICTURES ENTERTAINMENT, INC.***		

Present: The Honorable	R. GARY KLAUSNER, U.S. DISTRICT JUDGE

Sharon L. Williams (Not Present)	Not Reported	N/A
Deputy Clerk	Court Reporter / Recorder	Tape No.

Attorneys Present for Plaintiffs:	Attorneys Present for Defendants:
Not Present	Not Present

Proceedings: **(IN CHAMBERS) Motion to Dismiss (DE 59)**

I. INTRODUCTION

On March 2, 2015, Michael Corona and eight other individuals ("Plaintiffs") filed a class action against Sony Pictures Entertainment, Inc. ("Sony"). The action arises out of a security breach wherein Sony's information technology infrastructure and network were hacked, and sensitive personal data of former and current Sony employees were stolen. Plaintiffs, all former employees of Sony, allege the following claims: (1) Negligence; (2) Breach of Implied Contract; (3) Violation of the California Customer Records Act; (4) Violation of the California Confidentiality of Medical Information Act; (5) Violation of the Unfair Competition Law; (6) Declaratory Judgment; (7) Violation of Virginia Code § 18.2-186.6; and (8) Violation of Colorado Revised Statutes § 6-1-716.

Currently before the Court is Sony's Motion to Dismiss. For the following reasons, the Court **grants in part** the motion.

II. FACTUAL BACKGROUND

Plaintiffs allege the following:

In November 2014, as a result of inadequate security measures, Sony was the victim of a cyber-attack, wherein Sony's information technology infrastructure and network were hacked. The perpetrators stole nearly 100 terabytes of data from Sony's system. Among the data was sensitive personal information of at least 15,000 current and former Sony employees. The information, which included financial, medical, and other personally identifiable information ("PII"), was used to threaten the individual victims and their families, and was posted on the internet. Because Sony was focused on

its own remediation efforts and not on protecting its former and current employees, Plaintiffs have had to purchase identity protection services and insurance, and take other measures to protect their compromised PII. Notwithstanding these measure, Plaintiffs face ongoing future vulnerability to identity theft, medical theft, tax fraud, and financial theft because their PII has been, and may still be, publicly available to anyone with an internet connection. In fact, Plaintiffs' PII has already been traded on black market websites and used by identity thieves.

III. JUDICIAL STANDARD

A. Rule 12(b)(1)

A party may move to dismiss for lack of subject matter jurisdiction under Rule 12(b)(1). When a defendant files a Rule 12(b)(1) motion, the plaintiff has the burden of establishing that the court has subject matter jurisdiction. *Kokkonen v. Guardian Life Ins. Co.* , 511 U.S. 375, 377 (1994). At the pleading stage, a plaintiff must meet this burden by alleging sufficient facts to show a proper basis for the court to assert subject matter jurisdiction over the action. Fed. R. Civ. P. 8(a)(1); *McNutt v. Gen. Motors Acceptance Corp.* , 298 U.S. 178, 189 (1936).

B. Rule 12(b)(6)

Under Federal Rule of Civil Procedure ("Rule") 12(b)(6), dismissal "is appropriate only where the complaint lacks a cognizable legal theory or sufficient facts to support a cognizable legal theory." *Mendiondo v. Centinela Hosp. Med. Ctr.*, 521 F.3d 1097, 1104 (9th Cir. 2008). 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 *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). A claim is facially plausible if the plaintiff alleges enough facts to draw a reasonable inference that the defendant is liable for the alleged misconduct. *Id.* A plaintiff need not provide detailed factual allegations but must provide more than mere legal conclusions. *Id.* "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Id.*

When ruling on a Rule 12(b)(6) motion, the court must accept the allegations in the complaint as true and construe them in the light most favorable to the non-moving party. *Cahill v. Liberty Mut. Ins. Co.*, 80 F.3d 336, 337–38 (9th Cir. 1996). Though the court generally cannot consider facts outside the complaint in ruling on a Rule 12(b)(6) motion to dismiss, *Arpin v. Santa Clara Valley Transp. Agency*, 261 F.3d 912, 925 (9th Cir. 2001), it may consider documents that are referenced in the complaint, *No. 84 Employer-Teamster Joint Council Pension Trust Fund v. Am. W. Holding Corp.*, 320 F.3d 920, 925 n. 2 (9th Cir. 2003).

IV. DISCUSSION

Sony argues that the Court has no subject matter jurisdiction over this action, as Plaintiffs lack Article III standing. Sony also argues that even if Plaintiffs have standing, their individual claims still fail pursuant to Rule 12(b)(6) because they have not stated any viable claim.

A. Standing

Article III of the U.S. Constitution limits the judicial power of the United States to cases and controversies. Article III has been interpreted to bar federal courts from exercising jurisdiction over suits raising "abstract questions" or claims "based merely on 'assumed potential invasions' of rights." *Ashwander v. Tenn. Valley Auth.* , 297 U.S. 288, 324-25 (1936). Federal courts police this limit on their

power through the doctrine of standing. *See, e.g., DaimlerChrysler Corp. v. Cuno* , 547 U.S. 332, 342 (2006). To have standing, a plaintiff must establish an injury-in-fact that is fairly traceable to defendant's conduct and that is likely to be redressed by the requested relief. *Lujan v. Defenders of Wildlife* , 504 U.S. 555, 560-61 (1992). In the absence of standing, there is no subject matter jurisdiction. *See Bender v. Williamsport Area School Dist* ., 475 U.S. 534, 546–47 (1986). It is well-established that the existence of subject matter jurisdiction is determined based on the state of things at the time the plaintiff brings the action. *Grupo Dataflux v. Atlas Global Group, L.P.*, 541 U.S. 567, 570 (2004).

Defendant argues that Plaintiffs lack standing because they fail to allege a current injury or a threatened injury is that certainly impending. The Court disagrees.

In *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010), a laptop containing personal identifying information of 97,000 employees had been stolen, and the Ninth Circuit was asked to address this very same issue. There, the court found that, where the information had already been stolen, allegations of increased risk of future identity theft were a credible threat of real and immediate harm. *Id*. at 1143. More recently, in *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013), the U.S. Supreme Court decided a case also involving threatened injury as the injury-in-fact. There, instead of using the phrase, "real and immediate harm," the Court stated that "allegations of possible future injury are not sufficient," and "threatened injury must be *certainly impending* to constitute injury in fact." *Id*. at 1141 (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990))(emphasis added). While the Court found no standing based on the facts before it, despite the slight difference in wording, the injury-in-fact standard remained unchanged. *See, e.g., In re Adobe Systems, Inc. Privacy Litig.*, 2014 WL 4379916, at *8 (N.D. Cal. Sept. 4, 2014).

Here, Plaintiffs have alleged that the PII was stolen and posted on file-sharing websites for identity thieves to download. (Am. Compl., ¶¶ 1, 22, 24-26, 29, 80, 86, 91, 98, 101, 107, 115, 122, and 128.) Plaintiffs also allege that the information has been used to send emails threatening physical harm to employees and their families. (Am. Compl., ¶¶ 1 and 27.) These allegations alone are sufficient to establish a credible threat of real and immediate harm, or certainly impending injury.

The Court finds that Plaintiffs have Article III standing to assert this action, and **denies** Plaintiff's motion to dismiss for lack of subject matter jurisdiction.

B. Sufficiency of Claims

Sony argues that even if Plaintiffs have standing, dismissal pursuant to Rule 12(b)(6) is appropriate, as they have failed to adequately alleged their claims. The Court addresses each claim in turn.

1. *Negligence*

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

Sony challenges this claim on two grounds: (1) Plaintiffs have not alleged any cognizable injury to support a claim for negligence; (2) the economic loss doctrine bars Plaintiffs claim.

a. *Cognizable Injury*

"It is fundamental that a negligent act is not actionable unless it results in injury to another." *Fields v. Napa Milling Co.*, 164 Cal. App. 2d 442 (1958). Moreover, "[n]ominal damages . . . cannot be recovered in a negligence action, where no actual loss has occurred." *Id*. California courts have indicated that speculative harm or the mere threat of future harm is insufficient to constitute actual loss. *Jordache Enters., Inc. v. Brobeck, Pheger & Harrison, et al*, 18 Cal. 4th 739 (1998).

Plaintiffs allege that Sony breached two separate duties: (1) the duty to implement and maintain adequate security measure to safeguard its employees' PII; and (2) the duty to timely notify Plaintiffs that their PII had been compromised. In the complaint, Plaintiffs do not clearly delineate the alleged injuries resulting from untimely notification versus inadequate security measures. Rather, Plaintiffs generally allege that as a result of Sony's breach of duties, Plaintiffs have suffered the following injuries: (1) loss of opportunity to control how their PII is used; (2) diminution in the value and/or use of their PII; (3) the compromise, publication, and/or theft of their PII; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft or unauthorized use of financial and medical accounts; (5) lost opportunity costs and loss of productivity from efforts to mitigate the actual and future consequences of the breach; (6) costs associated with the inability to use credit and assets frozen or flagged due to credit misuse; (7) unauthorized use of compromised PII; (8) tax fraud or other unauthorized charges to financial, health care or medical accounts; (9) continued risk to the PII that remain in the possession of Sony, as long as Sony fails to undertake adequate measures; and (10) future costs in terms of time, effort, and money that will be expended to prevent and repair the impact of the data breach. (Am. Compl. ¶ 146.)

To the extent Plaintiffs allege future harm or an increased risk in harm that has not yet occurred, those allegations do not support a claim for negligence, as they fail to allege a cognizable injury. Similarly, general allegations of lost time are too speculative to constitute cognizable injury. To the extent Plaintiffs' alleged injury relies on a theory that their PII constitutes property, those allegations also fail, as Plaintiffs have not provided any authority that an individual's personal identifying information has any compensable value in the economy at large. *See In re Jetblue Airways Corp. Privacy Litigation*, 379 F. Supp. 2d 299, 397 (2005).

However, among its allegations of injury, Plaintiffs allege costs already incurred, including costs associated with credit monitoring, password protection, freezing/unfreezing of credit, obtaining credit reports, and penalties resulting from frozen credit. (Am. Compl. ¶¶ 81, 87, 92, 97, 103, 109, 110, 114, 123, 129.) California courts have not considered whether, in the context of data breach cases, costs relating to credit monitoring or other prophylactic measures sufficiently support a negligence claim. However, California has examined this issue in the context of exposure to toxic chemicals. *See Potter v. Firestone Tire & Rubber Co.*, 6 Cal. 4th 965 (1993). Therefore, by way of analogy, the Court looks to those cases for guidance in how the California Supreme Court would rule in the data breach context.

In *Potter*, the court found that monitoring is compensable where evidence shows that the need for future monitoring is a reasonably certain consequence of the defendant's breach of duty, and that the monitoring is reasonable and necessary. *Id*. at 1006-1007. To determine the reasonableness and necessity of such monitoring the court considered five factors.[1] As adapted to the data breach context, those factors are: (1) the significance and extent of the compromise to Plaintiffs' PII; (2) the sensitivity

[1] The factors articulated by the *Potter* court are (1) the significance and extent of the plaintiff's exposure; (2) the toxicity of the chemicals; (3) the relative increase in the chance of onset of disease in the plaintiff as a result of the exposure, when compared to (a) the plaintiff's chances of developing the disease had he not been exposed, and (b) the chances of the public at large developing the disease; (4) the seriousness of the disease for which plaintiff is at risk; and (5) the clinical value of early detection and diagnosis. *Potter*, 6 Cal. 4th at 1008.

of the compromised information; (3) the relative increase in the risk of identity theft when compared to (a) Plaintiffs' chances of identity theft had the data breach not occurred, and (b) the chances of the public at large being subject to identity theft; (4) the seriousness of the consequences resulting from identity theft; and (5) the objective value of early detection. *See id.* at 1008.

Upon review of the allegations, the Court finds that the Complaint sufficiently alleges facts to support the reasonableness and necessity of Plaintiffs' credit monitoring. First, Plaintiffs allege that Sony's data breach resulted in the public disclosure of its employees' most sensitive, non-public PII, including Social Security numbers, employment files, salary and bank account information, health insurance and other medical information, names, home and email addresses, visa and passport numbers, and retirement plan data. (Am. Compl. ¶ 1.) These records were posted on file-sharing websites and traded on torrent networks. (Am. Comp. ¶¶ 1 and 24.) Social security numbers were copied more than 1.1 million times throughout the 601 files stolen from Sony. (Am. Compl. ¶ 26.) The hackers posted some of the PII with a message to Sony employees threatening to release even more of their PII. (Am. Comp. ¶ 28.) As to the risk of identity theft, it is reasonable to infer that the data breach and resulting publication of Plaintiffs' PII has drastically increased their risk of identify theft, relative to both the time period before the breach, as well as to the risk born by the general public. It is commonly known that the consequences resulting from identity theft can be both serious and long-lasting. Moreover, Plaintiffs have alleged the same. (Am. Compl. ¶¶ 69-70.) Lastly, allegations that some plaintiffs have already received notification of attempted identity theft highlight the value of early detection. (*See* Am. Compl. ¶¶ 82, 93, 98, 115, and 116.)

Based on the foregoing, the Court finds that Plaintiffs adequately allege a cognizable injury by way of costs relating to credit monitoring, identity theft protection, and penalties. However, looking to the facts alleged, the Court finds implausible any argument that Sony's alleged delay in notification proximately caused any of the economic injury discussed above. These injuries fail to constitute incremental harm suffered by Plaintiffs as a result of any delay. Rather, the only reasonable inference is that Plaintiffs suffered the alleged economic injuries as a result of the data breach itself. Therefore, at this juncture, the Court **dismisses the portion of the claim based Sony's alleged duty to timely notify**.

b. *Economic Loss Doctrine*

As Defendants point out, purely economic loss cannot be recovered on a negligence claim. *See Giles v. General Motors Acceptance Corp.*, 494 F.3d 865, 875 (9th Cir. 2007). However, an exception exists where a special relationship exists between the parties. *J'aire Corp. v Gregory*, 24 Cal. 3d 799, 804 (1979). Courts determine the existence of a special relationship based on the following six factors: (1) the extent to which the transaction was intended to affect the plaintiff; (2) the foreseeability of harm to the plaintiff; (3) the degree of certainty that the plaintiff suffered injury; (4) the closeness of the connection between the defendant's conduct and the injury suffered; (5) the moral blame attached to the defendant's conduct; and (6) the policy of preventing future harm. *Id*.

Here, Plaintiffs allege that to receive compensation and employment benefits, they were required to provide their PII to Sony. (Am. Comp. ¶¶ 78, 84, 90, 96, 100, 106, 112, 119, and 126.) Based on these allegations, there is no doubt that this "transaction" was intended to affect Plaintiffs. Plaintiffs also allege that based on prior data breaches at other Sony companies and audits of Sony's own security systems, specifically with regard to human resource records, it was foreseeable that a data breach would occur and that Plaintiffs' would suffer harm. (Am. Compl. ¶¶ 31-46, 51-52, 143, 146.) Nonetheless, Sony made a business decision to not expend the money needed to shore up its system, and instead to accept the risk of a security breach. (Am. Compl. ¶ 43.) As a result, of Sony's failure to maintain an adequate security system and timely notify Plaintiffs of the breach, Plaintiffs suffered the injury discussed in Section IV.B.1.a, above. (Am. Compl. ¶ 146.)

These allegations, taken as true, sufficiently establish a special relationship that provides an exception to the economic loss doctrine.

Based on the foregoing, the Court **denies** Sony's motion to dismiss Plaintiffs' Negligence claim as it pertains to the alleged breach of duty to maintain adequate security measures.

2. *Breach of Implied Contract*

Plaintiffs allege that when Sony failed to reasonably protect Plaintiffs' PII from unauthorized use and failed to timely notify Plaintiffs that their PII had been compromised, Sony breached their implied duty of good faith. Defendants argue that Plaintiffs have failed to adequately allege a contract in the first instance. Therefore, Plaintiffs' claim based on an implied covenant necessarily fails. The Court disagrees.

"An implied-in-fact contract requires proof of the same elements necessary to evidence an express contract: mutual assent or offer and acceptance, consideration, legal capacity and lawful subject matter." *Northstar Financial Advisors Inc. v. Schwab Investments*, 779 F.3d 1036, 1050-51 (9th Cir. 2015)(citation omitted). Here, Plaintiffs allege that Sony offered employment to Plaintiffs in exchange for compensation and other benefits. (Am. Comp. ¶ 158.) To receive such compensation and other benefits, Sony required Plaintiffs to provide their PII, including names, addresses, Social Security number, medical information, and other personal information. *Id*. These allegations satisfy the elements requisite to the existence of a contract.

It is well-established that every contract imposes an obligation of good faith and fair dealing between the parties in its performance and enforcement. The duty embraces, among other things, an implied obligation that neither party will do anything to injure or destroy the right of the other party to receive the benefits of the agreement. *Harm v. Frasher*, 181 Cal. App. 2d 405, 418 (1960). Its purpose is to protect the covenants or promises contained in the contract, not to protect some general public policy interest not directly tied to the contract's purpose. *Wolf v. Walt Disney Pictures and Television*, 162 Cal. App. 4th 1107, 1120 (2008). Moreover, California law makes clear that establishing breach of the implied covenant requires proof of a conscious and deliberate act, which unfairly frustrates the agreed common purpose of the agreement. *Claridge v. RockYou, Inc.*, 785 F. Supp.2d 855, 865 (N.D. Cal. 2011)(citing *Careau & Co. v. Security Pacific Business Credit, Inc.*, 222 Cal. App. 3d 1371, 1394 (1990).

Here, Plaintiff alleges that the parties entered into a contract of employment in exchange for compensation and other benefits. (Am. Comp. ¶ 158.) To receive compensation and other benefits, Plaintiffs were required to provide Sony their PII. *Id*. Plaintiffs adequately allege that Sony consciously and deliberately failed to maintain an adequate security system. (Am. Compl. ¶ 43.) However, there are no facts indicating that Sony's acts were intended to frustrate the agreed common purpose of the agreement, i.e., employment in exchange for compensation and benefits. In fact, the purported class includes members that were no longer employed by Sony at the time the data breach occurred.

The Court finds that Plaintiffs' allegations do not adequately plead a claim for breach of implied contract, nor do the facts suggest that Plaintiffs' can plausibly cure this defect. Therefore, the Court **grants without leave to amend** Sony's motion as to Breach of Implied Contract.

3. *California Customer Records Act*

California Civil Code § 1798.80, *et seq.*, ("California Customer Records Act" or "CRA") regulates businesses with regard to treatment and notification procedures relating to their customers' personal information. Violation of any of the provisions may result in civil damages or injunction. CRA §1798.84 (b) and (e).

Sony argues that Plaintiffs may not sue under the CRA because they are not "customers," within the meaning of the statute. The Court agrees.

§1798.84, which authorizes civil action for damages, limits such action to "any customer." As defined in § 1798.80, "'customer' means 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." CRA §1798.80(c)(emphasis added). The facts alleged in the complaint make clear that Plaintiffs are not customers within the meaning of the statute.

In opposition, Plaintiffs argue that (1) §1798.81.5 expressly applies the CRA to all California residents; and (2) while the statute limits recovery of damages to customers, it broadly allows for injunctive relief. Plaintiffs' arguments are unpersuasive. As to the first argument, while true that the intent of the CRA, stated in §1798.81.5(a)(1), refers to "California residents," the language must be considered in the context of the entire statute. *See Angelucci v. Century Supper Club*, 41 Cal. 4th 160, 168 (2007). Looking to the broader context, it is clear that the statute intends to protect California residents in their role customers. First and most obviously, the title of the statute is "California *Customer* Records Act." Second, all primary regulating provisions reference either customers or information that a business owns, licenses, or maintains. As discussed above, "customer" is narrowly defined. Moreover, §1798.81.5 states that the terms "own," "license," and "maintain" refer to personal information that a business retains as part of the business' internal *customer account*. CRA §1798.81.5(a)(2)(emphasis added). The complaint does not allege that any of the plaintiffs were Sony customers. As to Plaintiffs' second argument, Plaintiffs correctly point out that the provision authorizing injunctive relief failed to specify who may seek such relief. However, on its face, the provision limits the remedy to only those businesses who violate, or propose to violate, the statute. As already discussed, violating the regulating provisions involve failing to provide notice or mishandling information regarding customers. Nothing in Plaintiffs' complaint suggests that Sony violated any of these provisions.

Based on the foregoing, the Court finds that Plaintiffs' fails to state a claim for violation of the CRA. Moreover, the fact alleged do not suggest that Plaintiffs can plausibly cure the defects. Therefore, the Court **grants without leave to amend** Sony's motion as to Plaintiffs' CRA claim.

4. *California Confidentiality of Medical Information Act*

Under the California Confidentiality of Medical Information Act ("CMIA"), "[e]ach employer who receives medical information shall establish appropriate procedures to ensure the confidentiality and protection from unauthorized use and disclosure of that information." California Civil Code §36.20(a). §56.36(b) of the CMIA states, "any individual may bring action against any person or entity who has negligently released confidential information or records concerning him or her in violation of this part . . .." As explained by the California courts, the term "released" does not connote an affirmative act on the part of the employer. *Regents of the Univ. of California v. Superior Court*, 220 Cal. App.4th 549, 564-65 (2013); *Sutter Health v. Superior Court*, 227 Cal. App. 4th 1546, 1554-55 (2014). Where an employer negligently maintains confidential medical information, thereby allowing an unauthorized third person to access it, the employer may have negligently released the information within the meaning of the CMIA. *Id*. Where such violation has occurred, the remedies available include (1)

nominal damages of $1,000, which does not require a showing of actual damages;[2] and (2) the amount of actual damages, if any, sustained by the plaintiff. Cal. Civ. Code § 56.36(b)(1) and (2).

Here, Plaintiffs allege that Sony violated §56.20 by failing to maintain the confidentiality of their medical information and by failing to institute reasonable safeguards to protect their medical information from unauthorized use. (Am. Comp. ¶ 183.) As a result, Plaintiffs' sensitive medical information was released in the data breach. (Am. Compl. ¶ 186.) Sony has admitted to the compromise of such HIPAA protected health information. (Am. Compl. §§ 65 and 187.) This information includes details of an employee's child with special needs, a surgical procedure, speech therapy lessons, and other medical conditions such as premature births, cancer, kidney failure, and alcoholic liver cirrhosis. (Am. Compl. ¶ 30.)

Upon review of the allegations, the Court finds that Plaintiffs have adequately stated a claim for violation of the CMIA. The Court **denies** Sony's motion as to the CMIA claim.

5. *Unfair Competition Law*

Plaintiffs assert a claim under California Business and Professions Code §17200, *et seq*. ("Unfair Competition Law" or "UCL"), and requests injunctive and declaratory relief, and attorneys fees and costs.[3] Sony argues that the claim fails because Plaintiffs fail to allege both loss of money or property, and unlawful, unfair, or fraudulent conduct.

For the reasons discussed in the foregoing sections, the Court disagrees. As stated above, Plaintiffs' allegations, taken as true, sufficiently allege an injury-in-fact, as well as injury in the form of economic loss. Moreover, as Plaintiffs' Negligence and CMIA claims have survived dismissal, there are predicate claims that form the basis for Plaintiffs' UCL claim. Therefore, the Court **denies** Sony's motion as to Plaintiffs' UCL claim.

6. *Virginia Code § 18.2-186.6(B)*

Virginia Code §18.2-186.6(B) requires entities that possess computerized data, including personal information, to disclose without unreasonable delay any breach of its security system upon discovery or notification of the breach. Notice must go to the Office of the Attorney General and any affected resident of the Commonwealth of Virginia. The statute authorizes an individual to recover direct economic damages from an entity that has violated this statute. VA Code Ann. §18.2-186.6(I).

Plaintiffs allege that Sony violated this statute by failing to notify them for at least three weeks that their PII had been compromised. (Am. Compl. ¶ 67.) Specifically, Plaintiff Corona, a Virginia resident, discovered an unencrypted spreadsheet containing his PII online, before he received any notification from Sony, and before he had an opportunity to obtain identity protection services. (Am. Compl. ¶¶ 80-81.)

As discussed in Section IV.B.1.a, above, Plaintiffs have failed to plausibly allege any injury resulting from Sony's alleged untimely notification. Without an allegation of economic damages, the claim fails. Based on the facts alleged, the Court finds that Plaintiffs cannot plausibly cure this defect.

---

[2] The award of nominal damages is subject to the limitation set forth in Cal. Civ. Code §56.36(e)(1), which does not appear relevant in this case.

[3] Plaintiffs' complaint also requests restitution. (Am. Comp. ¶ 218.) However, in response to Sony's challenge to this claim, Plaintiffs state among other things, that they do not intend to seek restitution. (Pls.' Opp'n, p. 19, fn 6.) Therefore, the Court deems any claim for restitution under the UCL waived.

Therefore, the Court **grants without leave to amend** Sony's motion as to Plaintiffs' Virginia statutory claim.

7. *Colorado Consumer Protection Act*

Similar to the Virginia statute, the Colorado Consumer Protection Act requires an entity that has suffered a data breach that compromises personal information to give notice to any affected Colorado resident as soon as possible. Colo. Rev. Stat. Ann. §6-1-716(2).

As Sony points out, the statute does not explicitly provide a private right of action, but rather vests enforcement powers in the attorney general. Plaintiffs cites to Colorado case law to support their argument that a private right of action is implied by the statute's text. Generally, taking into consideration the statutory language and context, courts presume that the legislature says in a statute what it means, and means in a statute what it says there. *See McDonald v. Sun Oil Co.*, 548 F.3d 774, 780 (9th Cir. 2008). This canon of statutory interpretation tends to guide the Court toward a finding of no private right of action. However, the Court need not address this particular issue. As the Court has previously found, Plaintiffs have not alleged direct economic damages resulting from Sony's allege failure to timely notify. As such, this claim fails.

The Court **grants without leave to amend** Sony's motion as to Plaintiffs' Colorado statutory claim.

8. *Injunctive Relief and Declaratory Judgment*

Sony argues that Plaintiffs are not entitled to injunctive or declaratory relief because they have alleged only retrospective injury for which damages would be sufficient to compensate. At this stage of litigation, particularly in light of Plaintiff's allegations and the Court's ruling on their UCL claim, it is premature to bar Plaintiffs from seeking these remedies.

The Court **denies** Sony's motion as to Plaintiffs' claim for Declaratory Judgment.

V. CONCLUSION

For the foregoing reasons, the Court grants in part Sony's motion. Specifically, the Court **denies** Plaintiff's motion to dismiss for lack of subject matter jurisdiction. The Court **grants without leave to amend** as to the following claims: (1) Breach of Implied Contract; (2) Violation of the California Customer Records Act; (3) Violation of Virginia Code §18.2-186.6(B); and (4) Violation of the Colorado Consumer Protection Act. Furthermore, the Court **dismisses** the portion of Plaintiffs' Negligence claim that alleges breach of the duty to timely notify. The Court **denies** as to the following claims: (1) Negligence (based on breach of the duty to maintain adequate security measures); (2) Violation of the CMIA; (3) Violation of the UCL; and (4) Declaratory Judgment.

IT IS SO ORDERED.

_____ : _____

Initials of Preparer