Alan CLARIDGE, Plaintiff,

v.

ROCKYOU, INC., Defendant.

No. C 09–6032 PJH.

United States District Court,
N.D. California.

April 11, 2011.

Background: User brought action against developer of online services and applications for use with social networking sites, alleging that developer failed to secure and safeguard its users' sensitive personally identifiable information (PII), including e-mail addresses, passwords, and login credentials. Developer moved to dismiss.

Holdings: The District Court, Phyllis J. Hamilton, J., held that:

(1) user failed to allege loss required to state a claim for violation of California's Unfair Competition Law (UCL);

(2) developer did not fall within scope of liability contemplated by California statute prohibiting any person from providing or assisting in providing a means of accessing a computer;

(3) user stated claims for breach of contract and breach of implied contract;

(4) developer's alleged failure to secure users' PII did not amount to breach of implied covenant of good faith and fair dealing; and

(5) user stated a negligence claim.

Motion granted in part and denied in part.

1. Federal Civil Procedure ⚿1744.1

At motion to dismiss stage, allegations of unauthorized disclosure of personal information were sufficient to plead injury in fact, as required for user to have Article III standing to sue developer of online services and applications for use with social networking sites, for failing to secure and safeguard its users' sensitive personally identifiable information (PII), including e-mail addresses, passwords, and login credentials. U.S.C.A. Const. Art. 3, § 2, cl. 1.

2. Antitrust and Trade Regulation ⚿290

User failed to allege any loss of money or property as a result of allegedly unfair competition on part of developer of online services and applications for use with social networking sites, as required to state a claim for violation of California's Unfair Competition Law (UCL) based on developer's alleged failure to secure and safeguard its users' sensitive personally identifiable information (PII), including e-mail addresses, passwords, and login credentials; even if user's PII constituted money or property, it was not lost because it did not cease to belong to him, or pass beyond his control. West's Ann.Cal.Bus. & Prof.Code § 17200 et seq.

3. Antitrust and Trade Regulation ⚿135(2)

Generally speaking, "unlawful practices" within the meaning of California's Unfair Competition Law (UCL) are any activities that are forbidden by law. West's Ann.Cal.Bus. & Prof.Code § 17200 et seq.

See publication Words and Phrases for other judicial constructions and definitions.

4. Antitrust and Trade Regulation ⚿135(1)

For purposes of California's Unfair Competition Law (UCL), "unfair acts" are those that offend an established public policy or are immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers. West's Ann.Cal.Bus. & Prof. Code § 17200 et seq.

See publication Words and Phrases for other judicial constructions and definitions.

5. Antitrust and Trade Regulation ⚿136

Federal Civil Procedure ⚿636

Fraud is not an essential element of a claim under California's Unfair Competition Law (UCL), although allegations of fraudulent conduct must nevertheless satisfy the heightened pleading requirements of rule requiring that, in all averments of fraud or mistake, the circumstances constituting fraud or mistake be stated with particularity. Fed.Rules Civ.Proc.Rule 9(b), 28 U.S.C.A.; West's Ann.Cal.Bus. & Prof.Code § 17200 et seq.

6. Antitrust and Trade Regulation ⚿290

To pursue either an individual or a representative claim under California's Unfair Competition Law (UCL), a plaintiff must have suffered an injury in fact and lost money or property as a result of such unfair competition. West's Ann.Cal.Bus. & Prof.Code § 17200 et seq.

7. Antitrust and Trade Regulation ⚿238

Developer of online services and applications for use with social networking sites did not fall within scope of liability contemplated by California statute prohibiting any person from knowingly and without permission providing or assisting in providing a means of accessing a computer, computer system, or computer network, where it took no active role in tampering with, or in gaining unauthorized access to computer systems; rather, it allegedly failed to secure and safeguard its users' sensitive personally identifiable information (PII) from third-party hackers. West's Ann.Cal.Penal Code § 502(c)(6).

8. Antitrust and Trade Regulation ⚿141

User failed to allege that he was a consumer, as required to state a claim against developer of online services and applications for use with social networking sites under California's Consumer Legal Remedies Act (CLRA) based on developer's alleged failure to secure and safeguard its users' sensitive personally identifiable information (PII), including e-mail addresses, passwords, and login credentials; user did not purchase or lease any goods or services from developer. West's Ann. Cal.Civ.Code § 1770(a)(5).

9. Telecommunications ⚿1340.5

Under California law, user sufficiently alleged a general basis for damages by alleging that failure to secure and safeguard his sensitive personally identifiable information (PII) on part of developer of online services and applications for use with social networking sites caused him to lose some ascertainable but unidentified value and/or property right inherent in the PII, as required to state claims against developer for breach of contract, breach of implied contract, and breach of implied covenant of good faith and fair dealing.

10. Contracts ⚿337(3)

Under California law, as a general matter, a plaintiff must plead damages resulting from any alleged contractual breach.

11. Contracts ⚿337(3)

The damage element inherent in contractual claims under California law parallels the type of concrete, non-speculative injury that must be pled in order to adequately allege injury in fact under Article III. U.S.C.A. Const. Art. 3, § 2, cl. 1.

12. Telecommunications ⚿1340.5

Privacy policy maintained by developer of online services and applications for use with social networking sites, providing that no liability would result due to a third party's unauthorized access of provider's secured computer system, did not preclude user's claims for breach of contract, breach of implied contract, and breach of implied

covenant of good faith and fair dealing, where user was alleging that developer's servers were not, in fact, secure.

13. Telecommunications ⚿1340.5

Under California law, alleged failure on part of developer to secure and safeguard its users' sensitive personally identifiable information (PII) did not amount to a breach of the implied covenant of good faith and fair dealing, absent any allegation that developer's failure was consciously and deliberately executed.

14. Negligence ⚿202

Under California law, an action in negligence requires a showing that the defendant owed the plaintiff a legal duty, that the defendant breached the duty, and that the breach was a proximate or legal cause of injuries suffered by the plaintiff.

15. Negligence ⚿259, 1591

Under California law, the doctrine of negligence per se is based on the rule that a presumption of negligence 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 that the plaintiff suffered as a result of the violation.

16. Negligence ⚿259

Under California law, a party who seeks to prevail on a cause of action premised on the negligence per se doctrine must establish, among other elements, that the party is one of the class of persons for whose protection the statute, ordinance, or regulation was adopted.

17. Telecommunications ⚿1341, 1346

Under California law, user sufficiently alleged damages element of negligence claim against developer of online services and applications for use with social networking sites, based on developer's failure to secure and safeguard its users' sensitive personally identifiable information (PII), including e-mail addresses, passwords, and login credentials, by alleging that he was injured by developer's actions permitting unauthorized and public disclosure of his PII, which had some unidentified but ascertainable value.

David Christopher Parisi, Suzanne L. Havens Beckman, Parisi & Havens LLP, Sherman Oaks, CA, Benjamin Harris Richman, Christopher Lilliard Dore, Jay Edelson, Michael James Aschenbrener, Edelson McGuire, LLC, Chicago, IL, for Plaintiff.

Daniel Justin Weinberg, Orrick Herrington & Sutcliffe LLP, Menlo Park, CA, Karen G. Johnson–McKewan, Orrick Herrington & Sutcliffe LLP, San Francisco, CA, for Defendant.

ORDER GRANTING IN PART AND DENYING IN PART MOTION TO DISMISS

PHYLLIS J. HAMILTON, District Judge.

Defendant's motion to dismiss the complaint came on for hearing on February 2, 2011 before this court. Plaintiff Alan Claridge ("plaintiff" or "Claridge"), appeared through his counsel, Christopher Dore and Michael Aschenbrener. Defendant RockYou, Inc. ("defendant" or "RockYou") appeared through its counsel, Daniel Weinberg, and Karen Johnson–McKewan. Having read all the papers submitted and carefully considered the relevant legal authority, the court hereby GRANTS defendant's motion to dismiss in part and DENIES the motion to dismiss in part, for the reasons stated at the hearing, and as follows.

BACKGROUND

Plaintiff brings the instant action against defendant for allegedly failing to secure and safeguard its users' sensitive personally identifiable information ("PII"), including email addresses, passwords, and login credentials for social networks like MySpace and Facebook. *See* First Amended Complaint ("FAC"), ¶ 1.

Defendant RockYou is a publisher and developer of online services and applications for use with social networking sites such as Facebook, MySpace, hi5 and Bebo. Applications developed by RockYou include those that enable users to share photos, write special text on a friend's page, or play games with other users. FAC, ¶ 10. Customers sign up to use RockYou's applications through rockyou.com, and they are asked to provide a valid e-mail address and registration password, which RockYou then stores in its database. FAC, ¶ 11. Additionally, a customer may be required to provide RockYou with a username and password for accessing a particular social network. *Id.* When users operate a RockYou application on a social networking site, RockYou utilizes the application as a platform to display paid advertisements. *See* FAC, ¶ 10. Defendant claims to be the leading provider of social networking application-based advertising services, with more than 130 million unique customers using its applications on a monthly basis. *Id.*

Plaintiff Claridge was a registered account holder with RockYou during the relevant time period, having registered with RockYou on August 13, 2008. FAC, ¶ 52. He signed up to utilize a photo sharing application offered by defendant, and submitted his e-mail address and password to defendant in order to do so. *Id.* at ¶ 53.

Plaintiff alleges that RockYou promised through its website that it would safeguard its users sensitive PII, through a written policy that stated: "RockYou! uses commercially reasonable physical, managerial, and technical safeguards to preserve the integrity and security of your personal information . . ." FAC, ¶ 12. Despite this promise, plaintiff alleges that RockYou—which collects and stores millions of users' PII in a large-scale commercial database—stored all PII in "clear" or "plain" text, which means that RockYou utilized no form of encryption in order to prevent intruders from easily reading and removing users' PII. FAC, ¶ 15. The PII was therefore readily accessible to anyone with access to the database. *Id.*, ¶ 16.

Among the options available to protect its customers, plaintiff alleges that RockYou could have followed a commonly used method of protecting sensitive data that requires conversion and storage of a "hashed" form of a plain text password. Defendant failed, however, to use hashing, or any other common and reasonable method of data protection. FAC, ¶¶ 18–19. Plaintiff alleges that, by failing to secure its users' PII, RockYou made email account and social networking account access available to even the least capable hacker. *Id.*, ¶ 21.

On December 4, 2009, an online security firm called Imperva, Inc. ("Imperva") notified RockYou of a security problem with its SQL database (SQL is a database computer language designed for storing data in database management systems). Imperva specifically informed RockYou that it had become aware of a 'SQL injection flaw' in RockYou's system—which would allow a hacker to take advantage of web software to introduce malicious code into a company's network. FAC, ¶ 25. According to Imperva, hackers were regularly discussing RockYou's SQL injection vulnerability in underground hacker forums, and the fact that this vulnerability was being actively exploited. *Id.* Imperva allegedly believed that prior to warning

RockYou, it was likely that breaches had already occurred through RockYou's SQL injection flaw, and that RockYou users' webmail accounts had been accessed as a result of such breaches. *Id.*, ¶ 28.

Plaintiff alleges that knowledge and understanding of SQL injection flaws has been widespread for more than a decade, and that such flaws are easy to prevent and well known to any web developer handling a large-scale commercial website. *See* FAC, ¶ 27. However, because RockYou did not have proper security in place and failed to use commercially reasonable methods to prevent a well-known method of attack, its security flaw was being actively exploited and the contents of its database were known and being made public through underground hacker forums on or before November 29, 2009. *Id.*, ¶ 31.

After Imperva warned RockYou of its SQL injection flaw, RockYou issued a press release stating that RockYou had immediately brought down its site in response to the warning, and kept it down until a security patch was in place. FAC, ¶ 34. Plaintiff alleges, however, that RockYou did not in fact respond immediately to Imperva's warning, and waited at least one day to take action to repair the SQL vulnerability. *Id.*, ¶ 35.

In the time prior to fixing the SQL vulnerability flaw—and prior to Imperva's warning—plaintiff alleges that at least one confirmed hacker known as "igigi" accessed RockYou's database and accessed and copied the email and social networking login credentials of approximately 32 million registered RockYou users. FAC, ¶ 36.

In a statement issued after RockYou publicly announced the security breach, defendant acknowledged that one or more individuals had illegally breached its databases, and further acknowledged that at the time of the breach, the hacked database had not been up to date with regard to "industry standard security protocols." FAC, ¶ 41.

On December 15, 2009, plaintiff Claridge received an e-mail from RockYou informing him that his sensitive PII stored with RockYou may have been compromised through a security breach. *See* FAC, ¶ 54.

Based on the foregoing allegations, plaintiff filed the instant suit against RockYou, on behalf of himself and a class of similarly situated individuals, defined as: "All individuals and entities in the United States who had RockYou accounts in 2009." FAC, ¶ 55.

Plaintiff asserts the following nine causes of action against RockYou:

1. violation of the Stored Communications Act, 18 U.S.C. § 2702;
2. violation of California's Unfair Competition Law, Cal. Bus. & Prof.Code § 17200;
3. violation of California's Computer Crime Law, Cal.Penal Code § 502;
4. violation of the California Consumer Legal Remedies Act, Cal. Civ.Code § 1750;
5. breach of contract;
6. breach of the implied covenant of good faith and fair dealing;
7. breach of implied contracts;
8. negligence; and
9. negligence per se

See generally FAC.

Defendant now moves to dismiss all nine causes of action, for failure to state a claim.

DISCUSSION

A. Legal Standard

A motion to dismiss under Rule 12(b)(6) tests for the legal sufficiency of the claims alleged in the complaint. *Ileto v. Glock*,

Inc., 349 F.3d 1191, 1199–1200 (9th Cir. 2003). Review is limited to the contents of the complaint. *Allarcom Pay Television, Ltd. v. Gen. Instrument Corp.,* 69 F.3d 381, 385 (9th Cir.1995). To survive a motion to dismiss for failure to state a claim, a complaint generally must satisfy only the minimal notice pleading requirements of Federal Rule of Civil Procedure 8.

Rule 8(a)(2) requires only that the complaint include a "short and plain statement of the claim showing that the pleader is entitled to relief." Fed.R.Civ.P. 8(a)(2). Specific facts are unnecessary—the statement need only give the defendant "fair notice of the claim and the grounds upon which it rests." *Erickson v. Pardus,* 551 U.S. 89, 93, 127 S.Ct. 2197, 167 L.Ed.2d 1081 (2007) (citing *Bell Atlantic Corp. v. Twombly,* 550 U.S. 544, 555, 127 S.Ct. 1955, 167 L.Ed.2d 929 (2007)). All allegations of material fact are taken as true. *Id.* at 94, 127 S.Ct. 2197. However, 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." *Twombly,* 550 U.S. at 555, 127 S.Ct. 1955 (citations and quotations omitted). Rather, the allegations in the complaint "must be enough to raise a right to relief above the speculative level." *Id.*

A motion to dismiss should be granted if the complaint does not proffer enough facts to state a claim for relief that is plausible on its face. *See id.* at 558–59, 127 S.Ct. 1955. "[W]here the well-pleaded facts do not permit the court to infer more than the mere possibility of misconduct, the complaint has alleged-but it has not show[n] that the pleader is entitled to relief." *Ashcroft v. Iqbal,* 556 U.S. 662, 129 S.Ct. 1937, 1950, 173 L.Ed.2d 868 (2009).

In addition, when resolving a motion to dismiss for failure to state a claim, the court may not generally consider materials outside the pleadings. *Lee v. City of Los Angeles,* 250 F.3d 668, 688 (9th Cir.2001). There are several exceptions to this rule. The court may consider a matter that is properly the subject of judicial notice, such as matters of public record. *Id.* at 689; *see also Mack v. South Bay Beer Distributors, Inc.,* 798 F.2d 1279, 1282 (9th Cir. 1986) (on a motion to dismiss, a court may properly look beyond the complaint to matters of public record and doing so does not convert a Rule 12(b)(6) motion to one for summary judgment). Additionally, the court may consider exhibits attached to the complaint, *see Hal Roach Studios, Inc. v. Richard Feiner & Co., Inc.,* 896 F.2d 1542, 1555 n. 19 (9th Cir.1989), and documents referenced by the complaint and accepted by all parties as authentic. *See Van Buskirk v. Cable News Network, Inc.,* 284 F.3d 977, 980 (9th Cir.2002).

B. Analysis

Defendant's motion requires a straightforward analysis of each of the nine claims stated in plaintiff's complaint. As a preliminary matter, however, the court first turns its attention to the parties' standing arguments. Defendant, who challenges plaintiff's ability to adequately allege standing, appears to subsume within its arguments two different sub-arguments: plaintiff's ability to allege injury in fact standing (i.e., Article III standing); and plaintiff's ability to adequately allege the elements of injury in connection with the individual claims asserted against defendant.

[1] To the extent the former is at issue, the parties dispute whether plaintiff has sufficiently alleged any actionable harm or concrete, tangible, non-speculative harm or loss. *See, e.g., Lujan v. Defenders of Wildlife,* 504 U.S. 555, 560–61, 112 S.Ct. 2130, 119 L.Ed.2d 351 (1992) ("Injury in fact" requires damage to "a legally pro-

tected interest which is (a) concrete and particularized, and (b) actual or imminent, not conjectural or hypothetical"). Plaintiff generally alleges that defendant's customers, including plaintiff, "pay" for the products and services they "buy" from defendant by providing their PII, and that the PII constitutes valuable property that is exchanged not only for defendant's products and services, but also in exchange for defendant's promise to employ commercially reasonable methods to safeguard the PII that is exchanged. *See* FAC, ¶¶ 45–47, 49, 50. As a result, defendant's role in allegedly contributing to the breach of plaintiff's PII caused plaintiff to lose the 'value' of their PII, in the form of their breached personal data. *See, e.g., id.,* ¶ 91.

In the face of defendant's contention that these allegations are both insufficient and unprecedented in establishing either a concrete or non-speculative injury, plaintiff admits to advancing a novel theory of damages for which supporting case law is scarce. And indeed, the case law cited by the parties demonstrates no clearly established law regarding the sufficiency of allegations of injury in the context of the disclosure of online personal information. *See, e.g., Ruiz v. Gap, Inc.,* 540 F.Supp.2d 1121 (N.D.Cal.2008) (considering electronic theft of job applicants' personal information and social security numbers, and finding plaintiff's allegation of harm sufficient to allege "injury in fact" standing at pleading stage, even if not more particularized injury under specific causes of action); *Doe 1 v. AOL LLC,* 719 F.Supp.2d 1102 (N.D.Cal.2010) (finding sufficient allegations of injury, even under particularized injury requirements of specific causes of action).

On balance, the court declines to hold at this juncture that, as a matter of law, plaintiff has failed to allege an injury in fact sufficient to support Article III standing. Not only is there a paucity of controlling authority regarding the legal sufficiency of plaintiff's damages theory, but the court also takes note that the context in which plaintiff's theory arises—i.e., the unauthorized disclosure of personal information via the Internet—is itself relatively new, and therefore more likely to raise issues of law not yet settled in the courts. For that reason, and although the court has doubts about plaintiff's ultimate ability to prove his damages theory in this case, the court finds plaintiff's allegations of harm sufficient at this stage to allege a generalized injury in fact. If it becomes apparent, through discovery, that no basis exists upon which plaintiff could legally demonstrate tangible harm via the unauthorized disclosure of personal information, the court will dismiss plaintiff's claims for lack of standing at the dispositive motion stage.

Notwithstanding the court's conclusion that Article III standing has generally been adequately pled at this juncture, the court further concludes that plaintiff has nonetheless failed to allege the more particularized elements of injury with respect to several of plaintiff's numerous individual causes of action.

The court now turns to the sufficiency of plaintiff's allegations with respect to each individual claim asserted.

1. *Stored Communications Act ("SCA") (Claim 1)*

In response to defendant's motion to dismiss this claim, plaintiff concedes from the outset that his complaint has inadvertently alleged the wrong provision of the Stored Communications Act. Specifically, the complaint alleges a cause of action pursuant to section 2702(a)(3) of the Act, which prohibits the disclosure of qualifying information to government entities. FAC, ¶¶ 66–74. Since this provision does not reach the merits of the instant lawsuit,

plaintiff contends that he instead meant to allege a claim under section 2702(a)(1) of the Act, which provides that: "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service . . .". *See* 18 U.S.C. § 2702(a)(1).

In view of plaintiff's concession, defendant's motion to dismiss plaintiff's claim pursuant to section 2703(a)(3) of the SCA is GRANTED. Plaintiff is granted leave to amend the complaint, however, in order to state a proper claim pursuant to section 2702(a)(1). Although defendant has argued that even a claim brought pursuant to section 2702(a)(1) should be dismissed on grounds that the alleged login credentials stolen by hackers do not constitute "contents of a communication" that would be covered by the statute, and on grounds that plaintiff fails to allege that RockYou "knowingly divulge[d]" any communications to any person, the merits of these arguments are not properly before the court absent amendment.

2. *Unfair Competition Law ("UCL") (Claim 2)*

[2–6] "California's unfair competition statute prohibits any unfair competition, which means 'any unlawful, unfair or fraudulent business act or practice.' " *In re Pomona Valley Med. Group,* 476 F.3d 665, 674 (9th Cir.2007) (*citing* Cal. Bus. & Prof.Code § 17200, et seq.). Generally speaking, unlawful practices are any activities that are forbidden by law. *Samura v. Kaiser Found. Health Plan, Inc.,* 17 Cal. App.4th 1284, 1292, 22 Cal.Rptr.2d 20 (1993). Unfair acts are those that "offend[ ] an established public policy" or are "immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers." *Podolsky v. First Healthcare Corp.,* 50 Cal.App.4th 632, 647, 58 Cal.Rptr.2d 89 (1996). As for allegedly fraudulent practices, fraud is not an essential element of a claim under § 17200, although allegations of fraudulent conduct must nevertheless satisfy the heightened pleading requirements of Rule 9(b). *See Vess v. Ciba–Geigy Corp. USA,* 317 F.3d 1097, 1103–05 (9th Cir.2003) (the heightened pleading standards of Rule 9(b) apply to allegations of fraud and allegations that sound in fraud, including false misrepresentations). Furthermore, "to pursue either an individual or a representative claim under the California unfair competition law," a plaintiff "must have suffered an 'injury in fact' and 'lost money or property as a result of such unfair competition.' " *Hall v. Time Inc.,* 158 Cal.App.4th 847, 849, 70 Cal. Rptr.3d 466 (2008).

Defendant here asserts plaintiff has failed to allege any loss of money or property as a result of defendant's allegedly unfair competition. The court agrees. As defendant notes, the California appellate court has recently passed upon the meaning of 'lost money or property' under the UCL specifically. In *Silvaco Data Systems v. Intel Corp.,* 184 Cal.App.4th 210, 109 Cal.Rptr.3d 27 (2010), the court noted that the UCL's standing requirements "go[ ] farther than the federal authorities by requiring that the plaintiff also have 'lost money or property.' Ordinarily when we say someone has "lost" money we mean that he has parted, deliberately or otherwise, with some *identifiable sum* formerly belonging to him or subject to his control; it has passed out of his hands by some means, such as being spent or mislaid, or ceded in a gamble, bad loan, or investment. Similarly, when we say someone has "lost" property we mean that he has parted with some particular item of property he formerly owned or possessed; it has *ceased to belong to him,* or at least has passed beyond his control or ability to retrieve it." *See* 184 Cal.App.4th at 244, 109 Cal. Rptr.3d 27 (emphasis added).

Applying this heightened concept of injury under the UCL, plaintiff's claim that his PII constitutes lost 'money'—based on plaintiff's untested theory that PII constitutes 'currency'—strains the acceptable boundaries of 'injury' under the statute. Similarly, to the extent that plaintiff makes the equally untested claim that his PII constitutes 'property,' plaintiff makes no allegation—nor can he—that his PII was 'lost' in the sense understood under the UCL. For as defendant points out, plaintiff's PII—e.g., his login and password information—did not cease to belong to him, or pass beyond his control.

In sum, plaintiff has failed to plead the heightened degree of injury required under the UCL. The court need not therefore delve into an analysis of whether plaintiff has met the remaining substantive prongs of a UCL claim, but instead GRANTS defendant's motion to dismiss the plaintiff's UCL claim based on the injury requirement alone. Because plaintiff cannot cure the foregoing deficiencies, the dismissal is with prejudice.

3. *California Penal Code § 502 (Claim 3)*

[7] Cal.Penal Code § 502(c)(6) prohibits any person from committing the following act: "Knowingly and without permission provid[ing] or assist[ing] in providing a means of accessing a computer, computer system, or computer network in violation of this section." Defendant asserts that this claim fails, however, because defendant is not a proper defendant under this subsection, and because plaintiff fails to allege that he suffered any "loss" under this provision.

Defendant is correct that dismissal is warranted by reason of the former. Plaintiff argues that defendant "provided a means" for hackers to access defendant's computer system, by failing to establish commercially reasonable security methods to protect the PII on its system. Plaintiff further relies on his allegations that defendant's actions were knowing and "without permission," because plaintiff never gave defendant permission to provide its PII to any hackers. FAC, ¶ 96. Review of section 502(c), however—which, as a penal statute, is to be strictly construed—reveals that the legislature's intent in drafting the statute was to protect against "tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems." *See* Cal.Penal Code § 502(a). And while plaintiff is correct that this protection is broadly read to include protection for all—i.e., individuals, private companies, government entities—it is less than clear that the statute is meant to subject individuals or entities to liability who took no active role in tampering with, or in gaining unauthorized access to computer systems. Indeed, the relatively few cases interpreting the statute largely seek to impose liability against individuals or entities who are alleged to have actually participated in unauthorized 'hacking' or the unlawful disclosure of information. This scenario is distinguishable from the present action, in which plaintiff seeks to impose liability on defendant for *third party* hackers' unauthorized access of and tampering with defendant's system.

In the absence of case law submitted firmly suggesting liability over defendant on grounds that defendant failed to provide a sufficiently secure computer system, the court agrees with defendant that plaintiff has failed to allege that defendant falls within the scope of liability contemplated by section 502(c)(6). Accordingly, defendant's motion to dismiss this claim is GRANTED. The dismissal is with prejudice.

4. *Consumer Legal Remedies Act Claim (Claim 4)*

[8] Defendant asserts that plaintiff cannot state a valid claim under the Con-

sumer Legal Remedies Act ("CLRA"). The CLRA proscribes various practices that are deemed unfair and/or deceptive to consumers. In alleging that defendant violated the CLRA, plaintiff relies on Cal. Civ.Code § 1770(a)(5), which prohibits any person "in a transaction intended to result or which results in the sale or lease of goods or services to any consumer" from: "[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have or that a person has a sponsorship, approval, status, affiliation, or connection which he or she does not have."

Defendant here correctly argues that plaintiff cannot state a valid claim under this provision of the CLRA because he has not alleged that he is a "consumer" within the meaning of the statute. The CLRA permits "consumers" to file suit pursuant to section 1770 and further defines a "consumer" to be "an individual who seeks or acquires, by purchase or lease, any goods or services for personal, family, or household purposes." *See* Cal. CIv.Code § 1761(d). Plaintiff, however, does not fall under this definition, since he did not "purchase or lease" any goods or services from defendant—a strict requirement under the statute. To be sure, plaintiff relies on his oft-repeated theory that, because his PII has an "ascertainable value" and constitutes both currency and property, his transfer of PII information to defendant in exchange for free applications, constitutes a "purchase" or "lease" under the CLRA. However, this argument—and the more generalized notion that the phrase "purchase" or "lease" contemplates any less than tangible form of payment—finds no support under the specific statutory language of the CLRA, nor has plaintiff relied on any legal authority suggesting as much.

All of which requires the court to conclude that plaintiff has failed to allege the requisite "consumer" status under the CLRA, such that a viable claim under the Act may be stated. The court therefore GRANTS defendant's motion to dismiss plaintiff's CLRA claim. Since there are no allegations that would cure the foregoing deficiency, the dismissal is with prejudice.

5. *Contractual Claims (Claims 5–7)*

[9] Plaintiff alleges three contractual based claims: breach of contract, breach of implied contract; and breach of the implied covenant of good faith and fair dealing. *See* FAC, ¶¶ 110–133. Defendant challenges all contractual claims, in part, for failure to allege any actionable damages. Specifically, defendant asserts that plaintiff has failed to allege that the value of his PII has diminished as a result of defendant's actions, how the breach of his PII affects him, or any loss whatsoever.

[10, 11] As a general matter, defendant is correct that plaintiff must plead damages resulting from any alleged contractual breach. *See, e.g., First Comm. Mort. Co. v. Reece,* 89 Cal.App.4th 731, 745, 108 Cal.Rptr.2d 23 (2001) ("A claim for breach of contract under California law consists of the following elements: (1) the existence of a contract; (2) performance by the plaintiff; (3) breach by the defendant; and (4) damage resulting from the breach.") (emphasis added); *Patent Scaffolding Co. v. William Simpson Const. Co.,* 256 Cal. App.2d 506, 511, 64 Cal.Rptr. 187 (1967) ("A breach of contract without damage is not actionable."); *Gomez v. Lincare, Inc.,* 173 Cal.App.4th 508, 93 Cal.Rptr.3d 388 (2009) ("A cause of action for breach of implied contract has the same elements as does a cause of action for breach of contract, except that the promise is not expressed in words but is implied from the promisor's conduct."); *Rosenfeld v. JPMorgan Chase Bank, N.A.,* 732 F.Supp.2d 952 (N.D.Cal.2010) (setting

forth elements necessary to establish breach of the covenant of good faith and fair dealing in California, including requirement that plaintiff have been harmed by the defendant's conduct). Moreover, the damage element inherent in contractual claims parallels the type of concrete, non-speculative injury that must be pled in order to adequately allege injury in fact under Article III. *See, e.g., Buttram v. Owens–Corning Fiberglas Corp.,* 16 Cal.4th 520, 531 n. 4, 66 Cal.Rptr.2d 438, 941 P.2d 71 (1997) ("[T]o be actionable, harm must constitute something more than nominal damages, speculative harm, or the threat of future harm-not yet realized . . .").

For the reasons already noted at the outset, therefore, the court concludes that at the present pleading stage, plaintiff has sufficiently alleged a general basis for harm by alleging that the breach of his PII has caused him to lose some ascertainable but unidentified "value" and/or property right inherent in the PII. As such, the court declines to dismiss plaintiff's breach claims on grounds that plaintiff has failed to allege damages or harm as a matter of law.

[12] To the extent that defendant has also argued, moreover, that plaintiff's contractual claims should be dismissed because the provisions of the privacy policy maintained by defendant expressly provide that no liability will result due to a third party's unauthorized access of defendant's computer system, defendant's argument is unpersuasive. For as plaintiff points out, the policy upon which the parties rely actually provides that: "RockYou! . . . assumes no liability or responsibility for . . . (III) any unauthorized access to or use of our *secure servers* and/or any and all personal information and/or financial information stored therein . . .". *See* Mot. Dismiss at 19:26–20:2 (emphasis added). Since plaintiff is alleging that the servers were not, in fact, secure, this provision of the policy does not automatically preclude plaintiff's contract claims.

[13] However, to the extent defendant additionally argues that plaintiff's claim for breach of the implied covenant of good faith and fair dealing must fail pursuant to *Careau & Co. v. Security Pacific Business Credit, Inc.,* 222 Cal.App.3d 1371, 1395, 272 Cal.Rptr. 387 (1990), defendant's position is well taken. As *Careau* makes clear, plaintiff must allege more than a mere contractual breach, and must go further by alleging "a failure or refusal to discharge contractual responsibilities, prompted not by an honest mistake, bad judgment or negligence but rather by a conscious and deliberate act, which unfairly frustrates the agreed common purposes and disappoints the reasonable expectations of the other party thereby depriving that party of the benefits of the agreement." *Id.* Here, plaintiff has alleged defendant's failure "to take commercially reasonable steps to safeguard and secure" plaintiff's PII information, and defendant's failure "to promptly and sufficiently notify" plaintiff that his PII had been compromised. Plaintiff alleges only in the most conclusory terms that such failures were "consciously and deliberately" executed, but provides no supporting or factual allegations that adequately allege the type of conscious and deliberate acts that are contemplated by *Careau.* Plaintiff has also failed to adequately rebut defendant's argument on this point.

Accordingly, while the court is unpersuaded that dismissal of plaintiff's contractual claims for breach of contract and breach of implied contract is warranted and therefore DENIES the motion with respect to these two claims, the court agrees with defendant that plaintiff's claim for breach of the implied covenant of good faith and fair dealing is fatally deficient, and GRANTS the motion with respect to

that claim. Leave to amend is granted, however, so that plaintiff may re-allege any additional facts sufficient to state a proper claim, if available.

6. *Negligence Claims (Claims 8–9)*

[14–16] Defendant also contends that plaintiff's negligence and negligence per se claims fail to state valid claims. An action in negligence requires a showing that the defendant owed the plaintiff a legal duty, that the defendant breached the duty, and that the breach was a proximate or legal cause of injuries suffered by the plaintiff. *See United States Liab. Ins. Co. v. Haidinger–Hayes, Inc.,* 1 Cal.3d 586, 594, 83 Cal.Rptr. 418, 463 P.2d 770 (1970). As for negligence per se, this doctrine is based on "the rule that a presumption of negligence 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 that the plaintiff suffered as a result of the violation." *See Quiroz v. Seventh Ave. Center,* 140 Cal.App.4th 1256, 1285, 45 Cal.Rptr.3d 222 (2006). Therefore, a party who seeks to prevail on a cause of action premised on the negligence per se doctrine must establish, among other elements, that the party is "one of the class of persons for whose protection the statute, ordinance, or regulation was adopted."

[17] First, beginning with plaintiff's negligence claim, defendant again reiterates that plaintiff's negligence claim fails because plaintiff has failed to plead any sufficiently cognizable injuries to establish damages. *See, e.g., Ruiz v. Gap, Inc.,* 380 Fed.Appx. 689, 691 (9th Cir.2010) (noting that actual injury in negligence actions, under California law, requires concrete, non-speculative harm). For the reasons already stated, however, the court concludes that plaintiff's allegations that he was injured by defendant's actions in permitting the unauthorized and public disclosure of his PII, which had some unidentified but ascertainable value, are sufficient to allege an actual injury at this stage. Accordingly, the court DENIES defendant's motion to dismiss the negligence claim on this ground.

Second, and turning to plaintiff's negligence per se claim, defendant asserts that plaintiff has failed to establish that any statutory violation—under the Stored Communications Act, UCL, Penal Code § 502, or CLRA—has been sufficiently pled, such that a claim for negligence per se may be stated. As already stated elsewhere herein, each of these claims—with the exception of plaintiff's SCA claim—has been dismissed with prejudice. Plaintiff has been given leave, however, to amend his SCA claim. Accordingly, since plaintiff's negligence per se claim may yet be premised upon a viable claim under the SCA, the court DENIES defendant's motion to dismiss the negligence per se claim at this time.

C. Conclusion

For all the foregoing reasons, defendant's motion to dismiss plaintiff's complaint is GRANTED in part and DENIED in part. Specifically, the court dismisses plaintiff's first, second, third, fourth, and sixth causes of action. The dismissal is with prejudice as to plaintiff's second, third, and fourth causes of action, and leave to amend is granted with respect to plaintiff's first and sixth causes of action. The court denies dismissal, however, with respect to plaintiff's fifth, seventh, eighth, and ninth causes of action.

Plaintiff must file any amended complaint no later than May 11, 2011. Leave is not granted to add any additional claims.

IT IS SO ORDERED.