David C. Marcus (SBN 158704)
david.marcus@wilmerhale.com
Christopher T. Casamassima (SBN 211280)
chris.casamassima@wilmerhale.com
WILMER CUTLER PICKERING
HALE AND DORR LLP
350 South Grand Avenue, Suite 2100
Los Angeles, CA 90071
Telephone: (213) 443-5300
Facsimile: (213) 443-5400

William F. Lee (*pro hac vice*)
william.lee@wilmerhale.com
WILMER CUTLER PICKERING
HALE AND DORR LLP
60 State Street
Boston, MA 02109
Telephone: (617) 526-6000
Facsimile: (617) 526-5000

Noah Levine (*pro hac vice*)
noah.levine@wilmerhale.com
WILMER CUTLER PICKERING
HALE AND DORR LLP
7 World Trade Center
250 Greenwich Street
New York, NY 10007
Telephone: (212) 230-8800
Facsimile: (212) 230-8888

Attorneys for Defendant
SONY PICTURES ENTERTAINMENT INC.

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

Michael Corona and Christina Mathis, individually and on behalf of others similarly situated,

Plaintiffs,

vs.

Sony Pictures Entertainment Inc.,

Defendant.

Case No. 2:14-cv-09600 RGK SH

SONY PICTURES ENTERTAINMENT INC.'S MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF ITS MOTION TO DISMISS COMPLAINT PURSUANT TO FEDERAL RULES OF CIVIL PROCEDURE 12(b)(1) AND 12(b)(6)

Hearing Date:	March 16, 2015
Time:	9:00 a.m.
Courtroom:	850
Judge:	Hon. R. Gary Klausner

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

INTRODUCTION

In November 2014, Sony Pictures Entertainment Inc. ("SPE") was the victim of a criminal attack on its information technology infrastructure and network. Compl. ¶ 15. As the Complaint itself acknowledges, this cyber-attack was massive and unprecedented, with the intent to cause harm to SPE. *See id.* ¶¶ 1, 23-25. In December 2014, the United States government attributed this sophisticated and wide-ranging attack on SPE to North Korea. *See* Press Release, Federal Bureau of Investigation, Update on Sony Investigation (Dec. 19, 2014), *available at* http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.[1]

This case, and the related cases pending before the Court, arise from that cyber-attack. The plaintiffs, each a former employee of SPE, claim that their personally identifying information was disclosed by the perpetrators of the cyber-attack and assert a variety of claims predicated on that fact. Neither plaintiff, however, claims to have suffered any concrete injury. There are no allegations of identity theft, no allegations of fraudulent charges, and no allegations of misappropriation of medical information. Instead, the plaintiffs assert a broad range of common-law and statutory causes of action based on their alleged fear of

[1] *See also* Press Statement by the Secretary of State John Kerry, Condemning Cyber-Attack by North Korea (Dec. 19, 2014), *available at* http://www.state.gov/secretary/remarks/2014/12/235444.htm; Press Statement by Secretary of Homeland Security Jeh Johnson on Cyber Attack on Sony Pictures Entertainment (Dec. 19, 2014); *available at* http://www.dhs.gov/news/2014/12/19/statement-secretary-johnson-cyber-attack-sony-pictures-entertainment. Indeed, the FBI has stated not only that the cyber-attack was highly sophisticated, but that "'[t]he malware that was used would have gotten past 90 percent of the Net defenses that are out there today in private industry and [would have been] likely to challenge even state government.'" Yahoo! News, FBI Official Calls Sony Attackers "Organized," "Persistent" (Dec. 10, 2014), *available at* http://news.yahoo.com/video/fbi-official-calls-sony-attackers-183646783.html.

an increased risk of future harm, as well as expenses they claim to have incurred to prevent that future harm. Those allegations, however, fail as a matter of law to establish the plaintiffs' standing to sue. Nor do they suffice to establish the type of harm required to state their claims. The Complaint thus falls short of the basic requirement that a plaintiff suffer some concrete and particularized injury before he files suit.

While all of the plaintiffs' claims share this overarching flaw, each is deficient in its own right for additional reasons detailed below. For example, the plaintiffs' negligence claim fails because they have not alleged any legally cognizable harm and, in the absence of any claimed physical injury, the claim is also barred by the economic loss doctrine. The plaintiffs' statutory claims fare no better. The plaintiffs assert a claim under the California Customer Records Act, but the plaintiffs are former employees of SPE—not "customers." And the plaintiffs assert a claim under Virginia's Notification Statute, but the plain terms of that statute provide a remedy to only those who suffer harm as a result of a delay in notification of a data breach, and the plaintiffs fail to allege any such harm here. Finally, the plaintiffs' California Confidentiality of Medical Information Act claim fails because, among other reasons, they do not allege that SPE, as opposed to the attackers, affirmatively disclosed their medical information. The Court should dismiss the Complaint in its entirety.

SUMMARY OF PERTINENT FACTUAL ALLEGATIONS

The facts below are drawn from the Complaint, which SPE is legally required to accept as true for purposes of this motion only, and from public sources of which this Court can take notice for purposes of this motion to dismiss.

The Complaint alleges that the attackers, calling themselves the "Guardians of Peace" ("GOP"), deployed a destructive malware to take over SPE's networks. Compl. ¶ 15. The GOP claimed to have obtained internal SPE data, and threatened to "release the data . . . to the world." *Id.* In addition, the Complaint alleges that

on December 2, 2014, the GOP released certain stolen personal information of SPE employees. *Id.* ¶ 17. The Complaint further alleges that this information included names, birthdates, addresses, social security numbers, salaries, passport and visa information, medical information, and employment records. *Id.* ¶¶ 17-18. That same night, SPE sent an internal memorandum to current employees notifying them of the potential theft of their personal information and suggesting they sign up for identity theft monitoring services, which SPE would provide to them free of charge. *Id.* ¶ 20. By December 5, 2014, SPE learned that the stolen and released files also contained personal information of former employees. *Id.* ¶ 21. According to the Complaint, on December 8, 2014, SPE sent another notification letter to its employees regarding the cyber-attack that may have compromised their personal information. *Id.* ¶ 24. On December 12, 2014, SPE's vendor offered former employees information about how to sign up for identity theft protection at no charge. *Id.* ¶¶ 84,87.[2]

On December 15, 2014, the plaintiffs filed this putative class action lawsuit, purporting to represent current and former SPE employees in the United States whose personal information was compromised by the attack. Compl. ¶ 90. They assert four causes of action: a common-law claim for negligence; violation of the California Confidentiality of Medical Information Act, Cal. Civ. Code § 56 *et seq.*; violation of the California Customer Records Act, Cal. Civ. Code § 1798.80 *et seq.*; and violation of Virginia Code § 18.2-186.6. Compl. ¶¶ 98-137. None of the claims is premised on actual misuse of the plaintiffs' personal information; instead, they allege that they have suffered an increased risk of identity theft and incurred

[2] The plaintiffs dedicate paragraphs of the Complaint to detailing a 2011 breach of the PlayStation Network, suggesting that it should have put "Sony" on notice of vulnerabilities. Compl. ¶¶ 44-65. The plaintiffs' group pleading is impermissible and unfounded. The PlayStation Network is operated by Sony Network Entertainment International LLC, a wholly separate corporation from SPE.

costs of mitigating that risk through additional credit monitoring services that they elected to purchase because the services SPE offered were (according to them) insufficient. *Id.* ¶¶ 5, 88, 108, 123, 136.

ARGUMENT

"'[W]hen subject matter jurisdiction is challenged under Federal Rule of Procedure 12(b)(1), the plaintiff has the burden of proving jurisdiction in order to survive the motion.'" *Kingman Reef Atoll Invs., L.L.C. v. United States*, 541 F.3d 1189, 1197 (9th Cir. 2008); *see Spencer v. Kemna*, 523 U.S. 1, 10-11 (1998). Article III standing "cannot be 'inferred argumentatively from averments in the pleadings.'" *Spencer*, 523 U.S. at 10. Rather, to satisfy his burden, the plaintiff must "clearly . . . allege facts demonstrating that he is a proper party to invoke judicial resolution of the dispute." *Id.* at 11 (internal quotation marks omitted).

To survive a motion to dismiss under Rule 12(b)(6), the plaintiffs must allege "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). While the "plausibility standard is not akin to a 'probability requirement,'" there must be "more than a sheer possibility that a defendant has acted unlawfully." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). A pleading with "no more than conclusions" is "not entitled to the assumption of truth." *Id.* at 679. This "standard is particularly demanding in 'complex, large-scale' data breach class action litigation," *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.* ("*Sony II*"), 996 F. Supp. 2d 942, 972 (S.D. Cal. 2014) (quoting *Grigsby v. Valve Corp.*, No. C12-0553JLR, 2012 WL 5993755, at *4-6 (W.D. Wash. Nov. 14, 2012)), where baselessly alleging a fear of future harm in the wake of a criminal event is all too easy.

I. THE COMPLAINT MUST BE DISMISSED BECAUSE THE PLAINTIFFS HAVE NOT SUFFERED INJURY IN FACT AND DO NOT HAVE STANDING TO SUE

"To establish Article III standing, a plaintiff must show" that he has suffered an "injury in fact"—*i.e.*, "an injury that is concrete and particularized, and actual or imminent." *Alliance for the Wild Rockies v. U.S. Dep't of Agric.*, 772 F.3d 592, 598 (9th Cir. 2014). In *Clapper v. Amnesty International USA*, the Supreme Court "reiterated that threatened injury must be *certainly impending* to constitute injury in fact, and that [a]llegations of *possible* future injury are not sufficient." 133 S. Ct. 1138, 1147 (2013) (alteration in original; internal quotation marks omitted). The Court further made clear that a plaintiff cannot "manufacture standing merely by inflicting harm on [himself] based on . . . fears of hypothetical harm that is not certainly impending." *Id*. at 1151.

The Supreme Court's reasoning in *Clapper* applies directly to common allegations made in data-breach cases like this one. The plaintiffs in such cases contend they have standing to sue because they have suffered "an increased risk . . . of identity theft," *In re Science Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, No. MDL 2360, 2014 WL 1858458, at *6 (D.D.C. May 9, 2014), or were forced to incur "the cost involved in preventing future harm," *id.* at *7. *See also, e.g., Galaria v. Nationwide Mut. Ins. Co.*, 998 F. Supp. 2d 646, 653 (S.D. Ohio 2014) (alleging "increased risk of identity theft, identity fraud, or medical fraud"; "time" and "costs to mitigate those risks"). These types of allegations, courts routinely hold, do not satisfy the standard set forth in *Clapper*: "[S]ince *Clapper* was handed down . . . , courts have been even more emphatic in rejecting 'increased risk' as a theory of standing in data-breach cases . . . . After all, an increased risk or credible threat of impending harm is plainly different from certainly impending harm, and certainly impending harm is what the Constitution and *Clapper* require." *SAIC*, 2014 WL 1858458, at *8; *see also Galaria*, 998 F.

Supp. 2d at 657 ("[U]nder *Clapper*, more [than increased risk of harm] is required to show an injury is certainly impending."); *Polanco v. Omnicell, Inc.*, 988 F. Supp. 2d 451, 467-70 (D.N.J. 2013) (same).

The same rationale governs here. The plaintiffs allege they have incurred or will incur costs to monitor for identity theft and to mitigate the risk of future identity theft, and are exposed to a future risk of fraud and identity theft. Compl. ¶¶ 5, 108, 123, 136. Under *Clapper*, these allegations are insufficient to satisfy Article III standing. *See, e.g.*, *SAIC*, 2014 WL 1858458, at *6-8 (relying on *Clapper* to reject standing based on alleged "risk of identity theft" and "cost of credit monitoring and other preventative measures"); *Galaria*, 998 F. Supp. 2d at 656-57 (finding that, post-*Clapper*, "the increased risk that Plaintiffs will be victims of identity theft, identity fraud, medical fraud, or phishing at some indeterminate point in the future" along with "costs to mitigate" those same risks are insufficient injuries to create standing).

It makes no difference that the plaintiffs allege that data already has been posted on the Internet, thereby allegedly increasing the risk of future identity theft. What matters for standing purposes is whether the plaintiffs have suffered concrete, imminent injury—and they do not allege that they have. Thus, in *SAIC*, notwithstanding the fact that certain plaintiffs had standing to sue because "they ha[d] suffered actual identity theft," the court concluded that the remaining plaintiffs—who did not allege any actual identity theft—lacked standing to sue. *SAIC*, 2014 WL 1858458, at *6; *see also Tierney v. Advocate Health & Hosps. Corp.*, No. 13 CV 6237, 2014 WL 5783333, at *2 (N.D. Ill. Sept. 4, 2014) (while certain plaintiffs "were injured insofar as each was notified of fraudulent activity," others lacked standing where they "allege[d] only a speculative fear of harm that someone could have bought and sold their personally identifiable information and personal health information on the international cyber black market and thereby place[d] them at risk of identity theft, identity fraud, and medical fraud"). Here,

the plaintiffs do not allege that their identities have been stolen or that their personal information has otherwise been misused.

The plaintiffs will likely argue that two decisions by federal district courts in California demonstrate that, notwithstanding *Clapper*, allegations of an increased risk of identity theft and costs incurred to hedge against future harm can be sufficient to establish standing in data-breach cases. In *In re Adobe Systems, Inc. Privacy Litigation*, No. 13-CV-05226, 2014 WL 4379916 (N.D. Cal. 2014), and *Sony II*, 996 F. Supp. 2d 942, the courts concluded that they were bound by the Ninth Circuit's pre-*Clapper* decision in *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010), to hold that the plaintiffs' allegations of an increased risk of identity theft sufficed to establish standing, because Article III required only "'a credible threat of harm'" that is "'real and immediate,'" *id.* at 1143. But those decisions incorrectly apply both *Krottner* and *Clapper*.

Because the Ninth Circuit's decision in *Krottner* is "clearly irreconcilable" with the Supreme Court's decision in *Clapper*, this Court should follow the Supreme Court's later ruling. *See Miller v. Gammie*, 335 F.3d 889, 900 (9th Cir. 2003) (en banc). *Krottner*'s holding cannot be squared with the Supreme Court's holding that a threatened injury must be "'*certainly impending*,'" and that even an "objectively reasonable likelihood" of injury—*i.e.*, a credible threat of harm—is insufficient. *Clapper*, 133 S. Ct. at 1147. Courts outside the Ninth Circuit have repeatedly recognized as much. *See, e.g.*, *SAIC*, 2014 WL 1858458, at *8 (grouping *Krottner* with cases whose standards are "clearly not supportable" "after *Clapper*"); *Galaria*, 998 F. Supp. 2d at 656.

There is more. *Krottner* relied heavily on the Seventh Circuit's decision in *Pisciotta v. Old National Bancorp*, 499 F.3d 629 (7th Cir. 2007), which held that "plaintiffs whose data had been stolen but not yet misused had suffered an injury-in-fact sufficient to confer Article III standing." *Krottner*, 628 F.3d at 1142-43 (discussing *Pisciotta*, 499 F.3d at 634). But district courts in the Seventh Circuit—

which, like this Court, are obligated to follow circuit precedent in the absence of an intervening, irreconcilable Supreme Court decision—have dismissed data-breach cases on standing grounds under *Clapper*, with at least one court expressly concluding that *Pisciotta* is no longer good law after *Clapper*. *See Strautins v. Trustwave Holdings, Inc.*, 27 F. Supp. 3d 871, 879 (N.D. Ill. 2014) ("To the extent that *Pisciotta* stands for the proposition that a risk of future harm does not have to be 'imminent,' 'certainly impending,' or pose greater than an objectively reasonable likelihood of injury (the standard *Clapper* expressly rejected as inadequate), this Court cannot square it with *Clapper*.").[3]

Clapper governs here, and requires the plaintiffs to allege a threatened injury that is "'*certainly impending*.'" 133 S. Ct. at 1147. The plaintiffs have not done so. Thus, the plaintiffs lack Article III standing, and the Complaint should be dismissed.

[3] *See also Lewert v. P.F. Chang's China Bistro, Inc.*, No. 14-cv-4787, 2014 WL 7005097, at *3 (N.D. Ill. Dec. 10, 2014) (relying on *Clapper* to reject standing where "[p]laintiffs do not allege that identity theft has occurred; rather, they allege that identity theft *may* happen in the coming years"); *Tierney*, 2014 WL 5783333, at *2 (plaintiffs lacked standing under *Clapper* where they "allege only a speculative fear of harm" stemming from the "risk of identity theft, identity fraud, and medical fraud"); *In re Barnes & Noble Pin Pad Litig.*, No. 12-cv-8617, 2013 WL 4759588, at *4 (N.D. Ill. Sept. 3, 2013) (dismissing data-breach claims for lack of standing under *Clapper* without reference to *Pisciotta*). *But see Moyer v. Michaels Stores, Inc.*, No. 14 C 561, 2014 WL 3511500, at *5 (N.D. Ill. July 14, 2014); *cf. Remijas v. The Neiman Marcus Group LLC*, No. 14 C 1735, 2014 WL 4627893, at *2-5 (N.D. Ill. Sept. 16, 2014) (reconciling *Pisciotta* with *Clapper*, but finding that plaintiffs lacked standing).

II. THE PLAINTIFFS' NEGLIGENCE CLAIM FAILS

A. The Plaintiffs Fail To Plead Facts Sufficient To State A Claim For Negligence

1. The Plaintiffs Do Not Allege A Cognizable Injury

The plaintiffs assert a negligence claim based on SPE's alleged failure to (1) adequately secure their personally identifiable information, and (2) timely notify them of the cyber-attack. Compl. ¶¶ 99-100, 102. Neither plaintiff alleges that his or her identity has been stolen as a result of the cyber-attack; neither alleges that his or her financial accounts or medical history have been misused or otherwise affected. The plaintiffs claim only—at most—that they face a risk of future identity theft and that they have spent time and money to prevent such theft.

For many of the same reasons that the plaintiffs fail to establish standing, *see supra* Part I, they also fail to allege injury sufficient to state a claim for negligence.[4] "Under California law, appreciable, nonspeculative, present harm is an essential element of a negligence cause of action." *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*("*Sony I*"), 903 F. Supp. 2d 942, 962 (S.D. Cal 2012) (citing cases). But here, the plaintiffs allege only speculative

---

[4] Even if this Court concludes that *Krottner* remains good law on Article III standing after *Clapper*, the plaintiffs' negligence claim would still fail. As the Ninth Circuit explained in *Krottner*, the court's "holding that Plaintiffs-Appellants pled an injury-in-fact for purposes of Article III standing does not establish that they adequately pled damages for purposes of their state-law claims." 406 F. App'x 129, 131 (9th Cir. 2010). The court therefore affirmed dismissal of the plaintiffs' negligence claim because it was premised entirely on "the danger of future harm." *Id.* ("Even . . . the only plaintiff who claims his personal information has been misused[] alleges no loss related to the attempt to open a bank account in his name."); *see also In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 963 (S.D. Cal 2012) ("While Plaintiffs have currently alleged enough to assert Article III standing to sue based on an increased risk of future harm, the Court finds such allegations insufficient to sustain a negligence claim under California law.").

injuries, limited to "increased risk of fraud and identity theft" and costs they incurred to protect themselves against such risks. Compl. ¶¶ 5, 108. The plaintiffs do not allege that their identities have been stolen or their personal information used in any other fraud. The absence of any such allegations dooms their negligence claim. "In short, when personal information is compromised due to a security breach, there is no cognizable harm absent actual fraud or identity theft." *Grigsby*, 2012 WL 5993755, at *2.[5]

Courts in data-breach cases "routinely dismiss actions," where, as here, "the only damages a plaintiff alleges . . . are increased risk of identity theft and money spent on monitoring credit." *Grigsby*, 2012 WL 5993755, at *2 (dismissing negligence claim, among others); *see also Bell v. Blizzard Entm't, Inc.*, Case No. 2:12-cv-09475-BRO-PJW, Dkt. 54, at 13 (C.D. Cal. July 11, 2013) (under Delaware law, increased risk of future harm insufficient to state a negligence claim). In *Sony I*, for example, the plaintiffs brought a negligence claim, asserting that "they were injured because their Personal Information was stolen, which has exposed them to an increased risk of identity theft and fraud." 903 F. Supp. 2d at 962. They also sought to recover the cost of "credit monitoring" services incurred as a result of the perceived increased risk. *Id*. at 960. But "no Plaintiff allege[d] any identity theft or unauthorized use of his information causing a pecuniary loss." *Id*. at 962. The court thus dismissed the negligence claim for lack of injury: "[W]ithout specific factual statements that Plaintiffs' Personal Information has been misused, in the form of an open bank account, or un-reimbursed charges, the mere 'danger of future harm, unaccompanied by present damage, will not support a

[5] The plaintiff in *Grigsby* resided in California and the parties argued the case under California law. The court did not undertake a choice-of-law analysis, concluding that "it does not matter whether California or Washington law applies since the same result would follow under either." 2012 WL 5993755, at *2 n.1.

negligence claim.'" *Id.* at 963. Those allegations are absent here, too, so the negligence claim should be dismissed.

The plaintiffs' delayed-notification negligence theory fails for another reason. To state a claim based on SPE's allegedly delayed notice, the plaintiffs would have to plausibly allege that the injury they suffered was traceable not to the cyber-attack itself, but to SPE's alleged delay in notifying the plaintiffs of the attack. *See Sony II*, 996 F. Supp. 2d at 965 (requiring allegations of "cognizable injury proximately caused" by the delay itself). That is, they are required to allege "*incremental* harm as a result of the delay." *Adobe*, 2014 WL 4379916, at *10 (dismissing statutory notification-delay claim). The plaintiffs allege nothing of the sort. They say generically that SPE "breached its duties to timely and accurately disclose" the cyber-attack and, in conclusory fashion, that "[a]s a direct and proximate result of [SPE's] breach of its duties," the plaintiffs suffered harm. Compl. ¶¶ 107-08. That does not suffice under Rule 8. *See Iqbal*, 556 U.S. at 678 ("'formulaic recitation of the elements of a cause of action will not do'").

2. The Economic Loss Doctrine Bars The Plaintiffs' Negligence Claim

The plaintiffs' negligence claim is also barred by the economic loss doctrine. That doctrine "bars a plaintiff from recovering for purely economic losses under a tort theory of negligence." *In re Michaels Stores Pin Pad Litig.*, 830 F.Supp.2d 518, 528 (N.D. Ill. 2011). "It reflects the belief that tort law affords the proper remedy for loss arising from personal injury or damages to one's property, whereas contract law and the Uniform Commercial Code provide the appropriate remedy for economic loss stemming from diminished commercial expectations without related injury to person or property." *In re Target Corp. Customer Data Sec. Breach Litig.*, No. MDL 14-2522 PAM/JJK, 2014 WL 7192478, at *15 (D. Minn. Dec. 18, 2014); *see Aas v. Superior Ct. of San Diego Cnty.*, 12 P.3d 1125, 1150 (Cal. 2000), *superseded by statute on other grounds as noted in Rosen v. State*

Farm Gen. Ins. Co., 70 P.3d 351, 357 (Cal. 2003) (economic loss rule preserves distinction between tort and contract actions); *Seely v. White Motor Co.*, 403 P.2d 145, 151 (Cal. 1965) (in negligence, damages are "limited to . . . physical injuries and there is no recovery for economic loss alone").

The plaintiffs allege neither physical injury nor damage to property. Rather, the plaintiffs' claimed damages are purely economic—risk of economic losses from future identify theft and misuse of personal information and efforts to protect against the same. Compl. ¶¶ 5, 108. The claims are accordingly barred by the economic loss doctrine. *See also Sony II*, 996 F. Supp. 2d at 967-73 (dismissing California negligence claim under economic loss rule); *Target*, 2014 WL 7192478, at *16 (same); *Michaels*, 830 F. Supp. 2d at 530-31 (same, under Illinois law).[6]

III. THE PLAINTIFFS' STATUTORY CLAIMS FAIL

A. The Complaint Fails To State A Claim Under The California Customer Records Act Because Mathis Is Not A California "Customer" And Because She Has Not Suffered Cognizable Harm

Plaintiff Mathis's claim under the California Customer Records Act (the "CRA"), California Civil Code §§ 1798.80 *et seq.*, fails for at least three reasons.

---

[6] The plaintiffs' allegations that SPE should have been "on notice" of its alleged security vulnerabilities based on prior security incidents does not change this conclusion, nor does it suffice to render SPE's alleged conduct intentional. Plaintiffs frequently make these sorts of allegations in data-breach cases, and courts routinely dismiss their claims notwithstanding. *See, e.g., In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d at 530-31 (dismissing claims notwithstanding allegations defendant acted with reckless indifference to known security risks in light of similar security breach, and noting that allegations of "willful conduct" do not create an exception to economic loss rule); *Sony II*, 996 F. Supp. 2d at 968-69 (dismissing claims notwithstanding allegations that defendant was "reckless[]" in its approach to data security, and that known risk of prior security breaches created a special relationship for purposes of negligence claims).

First, Mathis may not sue under the CRA because she is not a "customer" within the meaning of the statute. As its title demonstrates, the California *Customer* Records Act provides relief to "[a]ny *customer* injured by a violation of this title." Cal. Civ. Code § 1798.84(b) (emphasis added). The term "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." *Id.* § 1798.80(c). Only a "customer" as defined by the statute may obtain relief—whether "damages, statutory penalties, or injunctive relief." *Boorstein v. CBS Interactive, Inc.*, 165 Cal. Rptr. 3d 669, 675 (Ct. App. 2013).

Mathis is a former employee, not a customer, of SPE. Compl. ¶¶ 12-13. She does not claim to have bought or leased anything from SPE. Indeed, she fails to allege that she is a "customer" entitled to relief under the CRA. *See id.* ¶¶ 116-124 (allegations under the CRA).

Second, Mathis's alleged injuries fall short of what the statute requires. Under the CRA, Mathis must plausibly allege that she was "injured" by SPE's conduct. Cal. Civil Code § 1798.84(b); *see also Boorstein*, 165 Cal. Rptr. 3d at 675 ("a plaintiff must have suffered a statutory injury to have standing to pursue a cause of action under" the CRA). As discussed above, her claimed injuries are purely speculative. Compl. ¶¶ 5, 123; *see supra* Part II.A.1.

Third, to the extent Mathis claims SPE delayed in notifying her of the cyber-attack, she fails to allege any causal link between that purported delay and any alleged harm. Indeed, the Complaint is totally silent on this score. *See Grigsby v. Valve Corp.* ("*Grigsby II*"), No. Civ. C12-cv-00553, Dkt. 51, slip op. 12 (W.D. Wash. Mar. 18, 2013) (dismissing analogous Washington state notification-delay claim where plaintiff failed to "allege facts supporting the claim that he was injured due to the interval between the hacking incident and [defendant's] notice of the incident and not just that he was injured by the hacking incident alone").

B. The Complaint Fails To State A Claim Under Virginia Code § 18.2-186.6(B) Because Corona Does Not Allege Any Injury Stemming From SPE's Alleged Failure To Notify

Plaintiff Corona claims that SPE violated Virginia Code § 18.2-186.6(B) (the "Virginia Statute") by failing to promptly disclose the cyber-attack. Compl. ¶¶ 92, 132, 136. That claim fails for the same reason that Mathis's claim under the analogous California CRA fails.

Corona says that he incurred "expenses for credit monitoring and identity theft protection," and spent hours safeguarding himself against possible identity theft in the future. Compl. ¶ 136. But Corona neglects to explain how this purported harm resulted from a delay in notification to him. Because Corona fails to connect SPE's purported notification delay with some incremental injury, the claim must be dismissed. *See, e.g.*, *Sony II*, 996 F. Supp. 2d at 1010 ("[P]laintiff must allege actual damages flowing from the unreasonable delay (and not just the intrusion itself) in order to recover actual damages."); *see also supra* Part II.A.1.

C. Plaintiffs Fail To State A Claim Under the CMIA

The plaintiffs' claim under the California Confidentiality of Medical Information Act ("CMIA") fails because the plaintiffs (1) do not adequately allege that any compromised information was "medical information" within the meaning of the statute; (2) do not allege that SPE affirmatively "disclosed" (Cal. Civ. Code § 56.36(b)) any medical information; (3) do not adequately specify any alleged deficiencies under the CMIA; and (4) fail to sufficiently allege any actual injury.

First, the CMIA defines "medical information" as "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment." Cal. Civ. Code § 56.05(j). The plaintiffs do not allege that the cyber-attack resulted in any such information about themselves having been stolen by the

responsible third parties here. The Complaint contains general allegations that stolen data included the "medical information" of some members of the putative class, Compl. ¶¶ 1, 3, 18, 114-15, but does not allege that *the plaintiffs'* medical information was stolen, nor that the information was "derived from" any of the sources identified in the statute. The plaintiffs' allegations are conclusory with no facts pled to support it or render it plausible.

Second, the plaintiffs' claim for unauthorized disclosure of their medical information under the CMIA fails because they have not alleged that SPE undertook an "affirmative act of communication" with respect to their medical information. *Regents of Univ. of Cal. v. Superior Ct.*, 163 Cal. Rptr. 3d 205, 216 (Ct. App. 2013), *as modified on denial of reh'g* (Nov. 13, 2013) (defining "disclosure" as used in CMIA § 56.10); *see also Sutter Health v. Superior Ct.*, 174 Cal. Rptr. 3d 653, 658-59 (Ct. App. 2014) (discussing *Regents*). Here, the plaintiffs concede that SPE did not take any affirmative act to communicate their medical information. To the contrary, the plaintiffs' own Complaint alleges that a third party—the so-called "GOP"—stole it. Compl. ¶ 18 ("[T]he hackers of Sony's Network had stolen . . . medical . . . information.").

Sutter Health is instructive. In that case, a thief stole medical records maintained by a group of health care providers. 174 Cal. Rptr. 3d at 656. The plaintiffs sued the providers for violating the CMIA by "disclos[ing]" their medical information. *Id*. These allegations did not state a claim under the CMIA, the Court of Appeal explained, because the defendant "did not intend to disclose the medical information to the thief, so there was no affirmative communicative act by [defendant] to the thief." *Id.* at 660. The plaintiffs' claims against SPE should be dismissed for the same reasons.

Third, the plaintiffs' claim for negligent release of their medical information under the CMIA fails because they do not adequately specify any alleged deficiencies under the statute. *See* Cal. Civ. Code § 56.20(a). To be sure, the

plaintiffs state in conclusory language that SPE acted negligently. Compl. ¶¶ 109-15. But they never explain what the statute required of SPE. Without any attempt to describe the confidential medical information at issue, or any alleged nexus between that information and the procedures that should have been in place to protect it, the plaintiffs' negligent-release claim fails.

Fourth, to the extent the plaintiffs seek to recover actual damages on their CMIA claims, they have failed to adequately allege a basis for such damages for the same reasons that the plaintiffs fail to allege any cognizable injury, described *supra* Part II.A.1, and their CMIA claim accordingly fails.

CONCLUSION

The plaintiffs lack standing, do not plead cognizable injury, and cannot sufficiently allege the elements of a viable claim against SPE. The Court should grant SPE's motion to dismiss.

DATED: February 9, 2015

Respectfully submitted,

By: /s/ *William F. Lee*
William F. Lee

WILMER CUTLER PICKERING
HALE AND DORR LLP

Attorneys for Defendant
SONY PICTURES ENTERTAINMENT INC.