

1 David C. Marcus (SBN 158704)  
david.marcus@wilmerhale.com  
2 Christopher T. Casamassima (SBN 211280)  
chris.casamassima@wilmerhale.com  
3 WILMER CUTLER PICKERING  
HALE AND DORR LLP  
4 350 South Grand Avenue, Suite 2100  
Los Angeles, CA 90071  
5 Telephone: (213) 443-5300  
6 Facsimile: (213) 443-5400

7 William F. Lee (*pro hac vice*)  
william.lee@wilmerhale.com  
8 WILMER CUTLER PICKERING  
HALE AND DORR LLP  
9 60 State Street  
Boston, MA 02109  
10 Telephone: (617) 526-6000  
11 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

12  
13 Attorneys for Defendant  
SONY PICTURES ENTERTAINMENT INC.  
14

15 **UNITED STATES DISTRICT COURT**  
16 **CENTRAL DISTRICT OF CALIFORNIA**

17 Michael Corona, Christina Mathis, et  
al., individually and on behalf of others  
18 similarly situated,

19 Plaintiffs,

20 vs.

21 Sony Pictures Entertainment Inc.,

22 Defendant.  
23

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

**SONY PICTURES  
ENTERTAINMENT INC.'S  
OPPOSITION TO PLAINTIFFS'  
MOTION FOR CLASS  
CERTIFICATION**

PUBLIC VERSION

Hearing Date: September 14, 2015  
Time: 9:00 a.m.  
Courtroom: 850  
Judge: Hon. R. Gary Klausner

**TABLE OF CONTENTS**

	<b>Page(s)</b>
BACKGROUND .....	1
I. THE CYBERATTACK AND SPE’S RESPONSE.....	1
II. PLAINTIFFS’ EXPERIENCES VARY WIDELY.....	2
III. THIS LITIGATION.....	5
ARGUMENT .....	5
I. NO CLASS CAN BE CERTIFIED ON THE NEGLIGENCE CLAIM.....	6
A. Individualized Issues Predominate With Respect To Injury.....	7
B. Individualized Issues Predominate With Respect to Causation.....	8
C. This Court Should Reject Certification Of Any Class Premised On A “Credit Monitoring” Theory.....	10
1. Individualized Issues Predominate With Respect To Claims For Prophylactic Measures .....	10
2. Differences In State Law Preclude Certification .....	15
II. NO CLASS CAN BE CERTIFIED ON THE CMIA CLAIM.....	16
III. NO CLASS CAN BE CERTIFIED ON THE UCL CLAIM .....	18
IV. NO CLASS CAN BE CERTIFIED ON DECLARATORY JUDGMENT ..	20
CONCLUSION.....	20

**TABLE OF AUTHORITIES**

**Page(s)**

**FEDERAL CASES**

1

2

3

4

5 *Amgen Inc. v. Connecticut Ret. Plans & Trust Funds,*  
133 S. Ct. 1184 (2013).....6

6

7 *Berger v. Home Depot USA, Inc.,*  
741 F.3d 1061 (9th Cir. 2014) .....19

8

9 *Campion v. Old Republic Home Protection Co.,*  
272 F.R.D. 517 (S.D. Cal. 2011) .....19

10

11 *Comcast Corp. v. Behrend,*  
133 S. Ct. 1426 (2013).....6

12

13 *Davis v. HSBC Bank, N.A.,*  
691 F.3d 1152 (9th Cir. 2012) .....20

14

15 *De La Torre v. CashCall, Inc.,*  
56 F. Supp. 3d 1105 (N.D. Cal. 2014).....20

16

17 *Farmer v. Phillips Agency, Inc.,*  
285 F.R.D. 688 (N.D. Ga. 2012) .....18

18

19 *Farrar & Farrar Dairy, Inc. v. Miller-St. Nazianz, Inc.,*  
254 F.R.D. 68 (E.D.N.C. 2008).....8

20

21 *Faulk v. Sears Roebuck & Co.,*  
2013 WL 1703378 (N.D. Cal. Apr. 19, 2013).....18

22

23 *Flores v. CVS Pharm., Inc.,*  
2010 WL 3656807 (C.D. Cal. Sept. 7, 2010) .....17

24

25 *Gartin v. S&M NuTec LLC,*  
245 F.R.D. 429 (C.D. Cal. 2007).....8

26

27 *Herskowitz v. Apple, Inc.,*  
301 F.R.D. 460 (N.D. Cal. 2014) .....20

28

29 *Ileto v. Glock Inc.,*  
349 F.3d 1191 (9th Cir. 2003) .....8

1 *In re GPU Antitrust Litig.*,  
 2 253 F.R.D. 478 (N.D. Cal. 2008) .....6  
 3 *In re Hannaford Data Breach Litig.*,  
 4 293 F.R.D. 21 (D. Me. 2013).....1, 7  
 5 *In re Rezulin Litig.*,  
 6 210 F.R.D. 61 (S.D.N.Y. 2002).....15  
 7 *In re St. Jude Med., Inc.*,  
 8 425 F.3d 1116 (8th Cir. 2005) .....12  
 9 *In re TJX Breach Litig.*,  
 10 246 F.R.D. 389 (D. Mass. 2007) .....1  
 11 *Lozano v. AT&T Wireless Servs., Inc.*,  
 12 504 F.3d 718 (9th Cir. 2007) .....20  
 13 *Mazza v. Am. Honda Motor Co.*,  
 14 666 F.3d 581 (9th Cir. 2012) .....16, 19  
 15 *Moore v. Apple Inc.*,  
 16 2015 WL 4638293 (N.D. Cal. 2015) .....6, 17  
 17 *Quezada v. Loan Ctr. of Cal., Inc.*,  
 18 2009 WL 5113506 (E.D. Cal. Dec. 18, 2009).....18  
 19 *Remijas v. Neiman Marcus Group*,  
 20 2015 WL 4394814 (7th Cir. 2015) .....9  
 21 *Ruiz v. Gap, Inc.*,  
 22 622 F. Supp. 2d 908 (N.D. Cal. 2009).....16  
 23 *Stollenwerk v. Tri-West Healthcare*,  
 24 254 F. App’x 664 (9th Cir. 2007).....13, 16  
 25 *Stollenwerk v. Tri-West Healthcare*,  
 26 No. 03-cv-185, Dkt. 139 (D. Ariz. June 10, 2008) (unpublished) .....1, 10, 16  
 27 *Stollenwerk v. Tri-West Healthcare*,  
 28 2005 WL 2465906 (D. Ariz. Sept. 6, 2005) .....13  
*Wal-Mart Stores, Inc. v. Dukes*,  
 131 S. Ct. 2541 (2011).....5, 8

**STATE CASES**

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

*Henry v. Dow Chem. Co.*,  
701 N.W. 2d 684 (Mich. 2005) .....15, 16

*In re Firearm Cases*,  
24 Cal. Rptr. 3d 659 (App. 2005).....19

*In re Hannaford Data Breach Litig.*,  
4 A.3d 492 (Me. 2010) .....6

*In re Tobacco II Cases*,  
46 Cal. 4th 298 (2009) .....18

*Lockheed Martin v. Sup. Ct.*,  
29 Cal. 4th 1096 (2003).....12

*Potter v. Firestone Tire Co.*,  
6 Cal. 4th 965 (1993).....5, 12, 13, 14

*Wood v. Wyeth-Ayerst Labs.*,  
82 S.W. 3d 849 (Ky. 2002).....16

1 Nearly nine months after the cyberattack on Sony Pictures Entertainment  
2 Inc., not one of the named plaintiffs has suffered any financial loss arising from an  
3 actual instance of identity theft. They nonetheless seek to certify a class of  
4 employees who they allege have been harmed through disclosure of their PII.  
5 Notwithstanding their heavy burden under Rule 23, Plaintiffs offer this Court no  
6 way to determine how this case could be tried as a class action.

7 Plaintiffs' refrain is that the issue of SPE's alleged breach of common-law  
8 and statutory duties is sufficiently common that class certification is warranted.  
9 But the question is whether common issues will predominate over individualized  
10 ones, and Plaintiffs make no showing that they will. Critically, Plaintiffs fail to  
11 show how liability could ever be adjudicated with generalized proof common to  
12 the class given that the elements of injury and causation, central to Plaintiffs'  
13 negligence and UCL claims, are entirely individualized. Nor have Plaintiffs shown  
14 how any entitlement to compensation for costs for credit monitoring or other  
15 prophylactic measures could be proven on a classwide basis. Finally, Plaintiffs  
16 offer no way of proving on a classwide basis that any health information disclosed  
17 for particular classmembers falls within the CMIA.

18 Plaintiffs cite no case certifying a class in a litigated data-breach case—nor  
19 could they. In each of the data-breach cases in which the issue was litigated in  
20 federal court, class certification was denied because plaintiffs failed to prove that  
21 common questions of injury or causation predominated over individualized ones.<sup>1</sup>  
22 Plaintiffs fail here, too, and certification should be denied.

## 23 **BACKGROUND**

### 24 **I. THE CYBERATTACK AND SPE'S RESPONSE**

25 The November 2014 cyberattack on SPE was an unprecedented attack on an  
26

---

27 <sup>1</sup> See *In re Hannaford Data Breach Litig.*, 293 F.R.D. 21 (D. Me. 2013);  
28 *Stollenwerk v. Tri-West Healthcare*, No. 03-cv-185, Dkt. 139 (D. Ariz. June 10,  
2008) (unpublished); *In re TJX Breach Litig.*, 246 F.R.D. 389 (D. Mass. 2007).

1 American company. Notwithstanding the FBI’s attribution of the attack to North  
2 Korea, as well as its conclusion that the highly sophisticated attack “would have  
3 gotten past 90% of the Net defenses” in place in private industry, Plaintiffs claim  
4 SPE is at fault and seek to hold it liable. Their creative account of the “[f]actual  
5 [b]ackground” of the cyberattack (Pls.’ Mem. 2-4)—which relies on uninformed  
6 media reports based on flatly untrue assertions, speculation, and multiple-level  
7 hearsay—is irrelevant here, and SPE emphatically denies it.

8 The perpetrators released SPE files onto the internet, some of which  
9 contained employees’ PII. Without regard to whether any individual’s PII was  
10 actually disclosed, SPE provided current and former employees with one year of  
11 identity theft repair services through AllClear ID, as well as the option to enroll in  
12 a premier credit and identity theft monitoring and remediation service (AllClear  
13 PRO) for one year—both free of charge. Ex. A, Turner Rep. ¶ 26.<sup>2</sup> AllClear PRO  
14 provides enrolled employees and their dependents with a \$1 million insurance  
15 policy (per individual) for reimbursement of actual costs and certain expenses  
16 incurred as a result of identity theft. *Id.*; Ex. B, Johnson Rep. ¶¶ 21-22.

## 17 **II. PLAINTIFFS’ EXPERIENCES VARY WIDELY**

18 As data breaches have become increasingly common, an empirical  
19 consensus has coalesced around certain critical facts—most relevant here, that  
20 individuals affected by a breach face a highly variable risk of identity theft and  
21 related injuries. As Plaintiffs’ own expert put it, there is a “whole bunch of  
22 variables” that make an individual “more likely to experience an identity theft  
23 crime, or less likely.” Ex. M, Ponemon Tr. 151. As SPE’s expert explains, those  
24 variables include (1) the type and particular combinations of information exposed;  
25 (2) the age of the information; (3) the person’s income and creditworthiness; and  
26 (4) the person’s practices with respect to their PII as well as their exposure to other

---

27 <sup>2</sup> All supporting materials, including the expert reports of Michael Turner and  
28 John Johnson, are submitted herewith as exhibits to the Casamassima Declaration.

1 data breaches. Ex. A, Turner Rep. ¶¶ 55-76. Whether that risk will ever  
2 materialize into an actual injury, and, if so, whether such injury bears any  
3 relationship to a particular data breach, are also highly variable. As SPE’s expert  
4 explains, injury is an exception rather than the rule. Most people whose data are  
5 exposed following a data breach never experience *any* data misuse. *Id.* ¶ 36. And  
6 of the small portion who do have their data misused, most do not suffer injury,  
7 because, among other reasons, their financial institutions compensate them for any  
8 losses. *Id.* ¶¶ 24, 36, 82.

9 Plaintiffs say this data breach is different from others—“unprecedented both  
10 in its breadth and the sensitive nature of the PII that was compromised and publicly  
11 revealed.” Pls.’ Mem. 1. That is not the case. For instance, Plaintiffs lean heavily  
12 on the fact that social security numbers (SSNs) were disclosed in the cyberattack,  
13 but in 2014 alone, 323 data breaches resulted in the disclosure of affected  
14 individuals’ SSNs; in fact, 51% of data breaches in the last five years have exposed  
15 SSNs. Ex. A, Turner Rep. ¶¶ 20, 47.

16 Plaintiffs’ experiences in the wake of the cyberattack are entirely consistent  
17 with the empirical consensus just discussed. To start, the PII disclosed for each  
18 Plaintiff varies widely.<sup>3</sup> Ex. A, Turner Rep. ¶¶ 57-64 & App’x A. For example,  
19 Mathis asserts only that her name, SSN, and former (not current) home address  
20 were disclosed. Ex. G, Mathis Tr. 53. (Even on that score, she appears to be  
21 wrong. Plaintiffs cite no evidence that her SSN was disclosed. The sole document  
22 they cite (at Ponemon Rep. 7 n.6) has the SSN of a *different* Mathis.) For his part,  
23

---

24 <sup>3</sup> Plaintiffs define the class by reference to “PII” (Pls.’ Mem. 6), but never say  
25 which information, specifically, qualifies one for inclusion in the class. It could be  
26 something as simple as a “name[],” or data like SSNs, or combinations of certain  
27 information (*id.* at 2). Plaintiffs do not say. The variation among the PII disclosed  
28 for each member of the proposed class is already critical to the motion presented  
here. *See infra* at 8-10, 12-15. The absence of any definition from Plaintiffs  
exacerbates the problem, and renders the class impossible to ascertain.



1 Forster believes an array of his PII was disclosed, including his SSN and birthday,  
2 as well as outdated bank information, an invalid driver’s license, and former  
3 medical insurance information (which he admits are “useless” or “worthless”). Ex.  
4 H, Forster Tr. 34-40. This same variation can be expected across the putative class.

5 What is more, some Plaintiffs maintain active online presences, which  
6 means that much of the PII they claim was disclosed in the cyberattack already had  
7 voluntarily been made available online. For example, while Forster complains that  
8 his title, place of work, and dates on which he joined and left SPE were disclosed,  
9 he acknowledges that he had posted that information to LinkedIn and thus could  
10 not be harmed by its disclosure. *Compare, e.g.,* Ex. C, Pls.’ Am. Interrog. Resps.  
11 10, *with* Ex. H, Forster Tr. 55-61. Levine likewise admits that he has “put a lot of  
12 [his] life online.” Ex. D, Levine Tr. 191. For him and others, a wide range of PII  
13 was available online prior to the attack. *See, e.g.,* Ex. E, Archibeque Tr. 45-54; Ex.  
14 H, Forster Tr. 55-61. Again, the same variations can be expected across the class.

15 [REDACTED]  
16 [REDACTED]  
17 Resps. 19-23; Ex. A, Turner Rep. ¶¶ 70-72 & tbl. 1. At least four may have  
18 [REDACTED]  
19 [REDACTED]

20 Springer Tr. 236-37. And an unknown number of putative classmembers—  
21 [REDACTED]  
22 [REDACTED]

23 Springer Tr. 141.

24 Plaintiffs identify a handful of what they consider to be illustrative examples  
25 of their injuries. But those examples confirm the variability (not to mention the  
26 weakness) of their claims. For instance, Shapiro claims that someone “tried” to  
27 make a large purchase using his credit card. Pls.’ Mem. 5. But he testified that  
28 (1) he had no idea whether SPE ever had his credit-card information, and could not

1 find that information disclosed on the internet, (2) no unauthorized withdrawal was  
2 actually made, and (3) any unauthorized withdrawal would have been reimbursed.

3 [REDACTED]

4 [REDACTED]

5 [REDACTED]

6 the cyberattack (Ex. F, Shapiro Tr. 61). Similarly, while Corona claims that  
7 somebody made an unauthorized purchase using his credit card after the  
8 cyberattack on SPE (for which he was fully reimbursed), he acknowledges that he  
9 also had unauthorized purchases on his credit card *before* the cyberattack, and that  
10 he could only “guess” at the connection, if any, between the more recent  
11 unauthorized purchase and the cyberattack. Ex. I, Corona Tr. 196-97, 202-04, 209-  
12 10. The best illustrations of injury Plaintiffs can marshal demonstrate no injury at  
13 all. Ex. A, Turner Rep. ¶¶ 94-102.

### 14 **III. THIS LITIGATION**

15 As relevant here, in ruling on SPE’s motion to dismiss, this Court held that  
16 Plaintiffs could not recover under their negligence claim for alleged injuries  
17 premised on “future harm or an increased risk in harm that has not yet occurred.”  
18 2015 WL 3916744, at \*4. Rather, Plaintiffs are limited to seeking recovery of  
19 “costs already incurred,” to the extent those costs are “reasonable and necessary,”  
20 *id.*, under a test adapted from *Potter v. Firestone Tire Co.*, 6 Cal. 4th 965 (1993).  
21 The Court also permitted Plaintiffs to pursue their CMIA claim; their UCL claim,  
22 to the extent “there are predicate claims that form the basis for” it; and their claims  
23 for declaratory and injunctive relief. 2015 WL 3916744, at \*8-9.

### 24 **ARGUMENT**

25 “Rule 23 does not set forth a mere pleading standard.” *Wal-Mart Stores, Inc.*  
26 *v. Dukes*, 131 S. Ct. 2541, 2551 (2011). Rather, Plaintiffs “must affirmatively  
27 demonstrate [their] compliance with the Rule.” *Id.* Here, Plaintiffs must prove  
28 that they are typical of the class and that “the questions of law or fact common to

1 class members predominate over any questions affecting only individual members.”  
 2 *Comcast Corp. v. Behrend*, 133 S. Ct. 1426, 1432 (2013). “Undertaking the  
 3 predominance analysis requires some inquiry into the merits, as the Court must  
 4 consider ‘how a trial on the merits would be conducted if a class were certified.’”  
 5 *Moore v. Apple Inc.*, 2015 WL 4638293, at \*9 (N.D. Cal. 2015). Where  
 6 “individualized inquiries ... would degenerat[e] into a series of individual trials on  
 7 issues material to any showing of liability,” no class can be certified. *Id.* at \*14.

### 8 **I. NO CLASS CAN BE CERTIFIED ON THE NEGLIGENCE CLAIM**

9 Plaintiffs say (at 11-12) that every element of their negligence claim—duty,  
 10 breach, causation, and injury—is susceptible to common proof. They focus,  
 11 however, on the first two elements and say virtually nothing about the latter two.  
 12 That omission is telling because without a showing of injury and causation, a  
 13 classmember has no negligence claim at all. *See In re Hannaford Data Breach*  
 14 *Litig.*, 4 A.3d 492, 496 (Me. 2010). If Plaintiffs cannot prove injury and causation  
 15 with “generalized proof ... applicable to the class as a whole,” *In re GPU Antitrust*  
 16 *Litig.*, 253 F.R.D. 478, 501 (N.D. Cal. 2008), then the question of liability would  
 17 ultimately devolve into thousands of mini-trials.<sup>4</sup>

18 Plaintiffs’ invocation of the medical-monitoring analogy does not change  
 19 things. Plaintiffs cite no case certifying a class seeking credit or medical  
 20 monitoring. Nor do they offer any method of proving here, on a classwide basis,  
 21

---

22 <sup>4</sup> *Amgen Inc. v. Connecticut Retirement Plans & Trust Funds*, cited by  
 23 Plaintiffs (at 10), has no application here. There, in a Rule 10b-5 case, the Court  
 24 found that if plaintiffs were wrong about their classwide proof of one element  
 25 (reliance), then it necessarily would result in a common classwide failure to prove  
 26 another element (materiality). In other words, there was no way in which the  
 27 “plaintiff class’s failure to prove an essential element of its claim for relief [would]  
 28 result in individual questions predominating over common ones.” 133 S. Ct. 1184,  
 1196 (2013). That is not the case here. Because there is a “fatal dissimilarity”  
 among class members,” *id.* at 1197, with respect to causation and injury, those  
 questions could never be resolved classwide, and predominance is absent.

1 that classmembers uniformly have incurred reasonable and necessary prophylactic  
2 costs. Instead, Plaintiffs say that classmembers are entitled to *future* credit-  
3 monitoring costs and that this alleged entitlement can be proved through  
4 generalized evidence, but they are wrong on that score too, and regardless, this  
5 Court’s order barred that relief.

6 **A. Individualized Issues Predominate With Respect To Injury**

7 As discussed, this Court limited Plaintiffs to recovery of certain “costs  
8 already incurred.” Plaintiffs offer *nothing* suggesting whether or how these  
9 injuries can be proven with common, classwide evidence—and they cannot.  
10 Instead, Plaintiffs give (at 5) individual examples of how some—but not all—of  
11 them claim to “have already been victims of identity fraud.” Specifically, they  
12 appear to seek recompense for the \$3,845.50 purchase on Corona’s credit card  
13 (even though it was reimbursed), and for Bailey and Archibeque’s PII having been  
14 made available for sale. Each of these claimed injuries involves different PII and  
15 different alleged harm, and thereby necessarily implicates evidence specific to each  
16 Plaintiff and each incident. Plaintiffs say *nothing* about how they might prove  
17 those injuries for *the class* through generalized proof. Indeed, their brief says  
18 nothing at all about putative classmembers’ injuries.

19 All Plaintiffs offer on this point is their expert’s promise that, “[t]o the  
20 extent putative class members suffer harm in the form of fraudulent financial  
21 charges for which they incur out-of-pocket damages, these damages could also be  
22 accounted for in my damages model.” Fishkind Rep. ¶ 18 n.8. The promise of an  
23 unspecified future expert opinion does not satisfy Plaintiffs’ burden on class  
24 certification. *See Hannaford*, 293 F.R.D. at 33.<sup>5</sup>

---

25  
26 <sup>5</sup> Plaintiffs say that *Hannaford* is distinguishable because they—unlike  
27 plaintiffs in that case—have provided expert testimony “on classwide damages.”  
28 Pls.’ Mem. 12. But they have not. Fishkind and Ponemon offer no way to test  
classwide injury or damages in a manner that takes account of the wide variation

1 Plaintiffs instead focus on the risk of *future* injury, saying that their experts  
2 have “explained that all class members will be subjected to heighte[ne]d *risk* of  
3 identity fraud *going forward for years to come*, and ... [have] provided an  
4 appropriate and common model for measuring the reasonable costs ... that class  
5 members *will incur* to monitor and protect themselves from identity fraud.” Pls.’  
6 Mem. 14-15 (emphasis added). But they again fail to demonstrate that they all  
7 suffered the same injury, warranting the same future relief. And in any event, this  
8 Court has already concluded that the risk of future fraud is not a “cost[] already  
9 incurred” and is not recoverable here. Even if it were, it could not be proven on a  
10 classwide basis, as discussed below. *See infra* Section I.C.1.

11 **B. Individualized Issues Predominate With Respect to Causation**

12 Plaintiffs’ entire argument on causation occupies one sentence: “Causation  
13 is also common to all class members in this case, since Plaintiffs allege that SPE’s  
14 failure to maintain adequate security was a substantial factor in causing their  
15 injury.” Pls.’ Mem. 12. That does not come close to satisfying their burden.  
16 Plaintiffs’ *allegations* are irrelevant at class certification, *Dukes*, 131 S. Ct. at 2551,  
17 and the one case they cite, *Ileto v. Glock Inc.*, 349 F.3d 1191, 1206-07 (9th Cir.  
18 2003), merely sets forth the causation standard for a negligence claim.

19 It is hardly surprising that Plaintiffs cite no case saying that causation can be  
20 proved on a common, classwide basis. Indeed, courts routinely *refuse* to certify  
21 negligence claims on the ground that “the proximate causation analysis involves  
22 individualized factual issues.” *Gartin v. S&M NuTec LLC*, 245 F.R.D. 429, 439  
23 (C.D. Cal. 2007) (collecting cases); *see Farrar & Farrar Dairy, Inc. v. Miller-St.*  
24 *Nazianz, Inc.*, 254 F.R.D. 68, 74 (E.D.N.C. 2008).

25 This case is no different. The causation inquiry for any classmember would  
26 first require analysis of the PII disclosed for that classmember in the cyberattack—

27  
28 among classmembers that they acknowledge is present here. *See generally* Ex. B,  
Johnson Rep. ¶¶ 57-78; Ex. A, Turner Rep. ¶¶ 55-76.

1 PII that varies among the classmembers. *See supra* at 3-4. To determine whether  
2 any particular injury to a classmember could have been caused by the cyberattack,  
3 the factfinder would then need to compare the disclosed PII to the information used  
4 in the particular, claimed identity fraud. Thus, even if the fraudulent charge on  
5 Corona’s credit card had resulted in financial loss to him (it did not), any causative  
6 link is negated because Corona admits that information about the affected account  
7 was not disclosed in the cyberattack. *See Ex. I, Corona Tr. 169, 199, 209-10.* That  
8 same inquiry would need to be conducted thousands of times for the putative class.

9 The factfinder would also have to consider each classmember’s history of  
10 identity theft and exposure to other data breaches. Plaintiffs (and, undoubtedly,  
11 unnamed classmembers) have been exposed to multiple breaches and incidents of  
12 identity theft involving various permutations of their PII. *See supra* at 4. To prove  
13 that any injury—or even risk of future injury—is attributable to the cyberattack,  
14 each classmember would have to show that *this* cyberattack, and not another event,  
15 caused any incident of identity fraud.<sup>6</sup> That issue is individualized, as Plaintiffs’

16 [REDACTED]  
17 [REDACTED]  
18 that *before* the cyberattack occurred, they experienced unauthorized credit-card  
19 charges and new account fraud similar to what they claim here. *See supra* at 5.  
20 Determining whether identity theft suffered by a classmember is attributable to the  
21 cyberattack, or instead to fraudsters in possession of classmembers’ PII for other  
22 reasons, requires an individualized inquiry; the question cannot be resolved

23  
24 <sup>6</sup> Plaintiffs may cite *Remijas v. Neiman Marcus Group*, 2015 WL 4394814, at  
25 \*7 (7th Cir. 2015), *reh’g pet. pending*, to argue that they do not have to make this  
26 showing. But *Remijas* addressed standing, not the proof necessary for a negligence  
27 claim. Notwithstanding *Remijas*, causation is still defeated by a showing that  
28 something other than the cyberattack was a more likely cause of a given instance  
of identity theft. *See id.* (defendants not liable where “their negligent actions were  
not the ‘but-for’ cause of the plaintiff’s injury”).

1 through generalized proof applicable to the class as a whole.

2 One of the few data breach cases to have addressed this question denied  
3 class certification on these exact grounds, concluding that “issues related to proof  
4 of causation would predominate over common questions.” *Stollenwerk*, Dkt. 139,  
5 at 7. Referring to an earlier decision in the same case, the court observed that the  
6 Ninth Circuit “focused on questions of fact individual to [plaintiff] that bore on  
7 causation,” including whether (and when) he had been the victim of prior incidents  
8 of identity fraud, whether “the type of information” disclosed in the breach “is the  
9 same kind needed to open credit accounts,” and his personal practices for  
10 maintaining his PII. *Id.* Because these “individualized issues related to proof of  
11 causation” were “personal to” the plaintiff, “and will not be true for other class  
12 members,” no class could be certified. *Id.*

13 That reasoning applies here as well. Plaintiffs have no way to prove at a  
14 class trial, through generalized evidence common to the class as a whole, that any  
15 injuries to classmembers were caused by the SPE cyberattack.

16 **C. This Court Should Reject Certification Of Any Class Premised**  
17 **On A “Credit Monitoring” Theory**

18 **1. Individualized Issues Predominate With Respect To Claims**  
19 **For Prophylactic Measures**

20 With respect to credit monitoring and other prophylactic measures, this  
21 Court permitted Plaintiffs to seek recovery of “costs already incurred,” to the  
22 extent those costs are “reasonable and necessary” under a five-factor test. Ignoring  
23 the Court’s limitation, Plaintiffs say that the class has been exposed to a common  
24 risk of *future* identity theft and that all classmembers are thus entitled to recover  
25 hypothetical *future* costs of credit monitoring. That is incorrect. As to  
26 prophylactic costs already incurred, the wide variation among Plaintiffs defeats  
27 their argument that they are each representative of the purported class; classwide  
28 injury cannot be proved by simply averaging their out-of-pocket expenses. More  
fundamentally, no class can be certified to seek prophylactic costs—already



1 incurred or future—because individualized issues predominate with respect to the  
2 reasonableness and necessity of those costs.

3 **a) Plaintiffs offer no method to prove classwide injury**  
4 **for costs already incurred**

5 Plaintiffs have not proposed any way to prove on a classwide basis that any  
6 prophylactic costs classmembers *already* incurred—by choosing to pay for a  
7 product rather than enroll in the AllClear product SPE provided free of charge—  
8 were “reasonable and necessary.” Many classmembers—including Forster—made  
9 the reasonable decision to enroll in AllClear and incur no additional expense for  
10 monitoring. Ex. B, Johnson Rep. ¶ 92. Other Plaintiffs—who were carefully  
11 chosen by their counsel out of more than 160 SPE employees interviewed<sup>7</sup>—  
12 enrolled in a range of products, with at least one Plaintiff buying, but never using,  
13 password-protection software (which does not protect her against the injuries  
14 Plaintiffs attribute to the cyberattack). Ex. G, Mathis Tr. 89. And Plaintiffs  
15 present no evidence about what, if anything, putative classmembers did on this  
16 score. To the extent Plaintiffs intend to prove that particular costs were even  
17 incurred by absent classmembers and that any such costs were reasonable and  
18 necessary for each such classmember, they confront a host of individualized  
19 questions: Was it reasonable for Springer to purchase LifeLock’s expensive  
20 Ultimate Plus product? For Archibeque to buy a less expensive LifeLock product?  
21 Was it necessary for Mathis to buy a product she never used? For Shapiro to  
22 freeze and unfreeze his credit numerous times? Ex. B, Johnson Rep. ¶¶ 76-77.

23 Nor does Plaintiffs’ expert have any model for measuring already incurred  
24 monitoring expenses *for the class*, again, to the extent classmembers even have  
25 incurred any. Fishkind’s “model” for determining those alleged damages is simply  
26 to average the costs claimed *by the eight Plaintiffs*, declare them “representative”

27 \_\_\_\_\_  
28 <sup>7</sup> Sarko Decl. ¶ 4 (ECF 32); Girard Decl. ¶ 4 (ECF 31-2); Sobol Decl. ¶ 8  
(ECF 31-3).



1 of the class, and allocate that “average” to each classmember as damages.  
2 Fishkind Rep. ¶¶ 17, 18 n.8, 27; Ex. L, Fishkind Tr. 56-57. That “model” ignores  
3 the expected variation among the class. Indeed, not even all Plaintiffs have  
4 incurred expenses. *See* Ex. L, Fishkind Tr. 56. For those who did, their alleged  
5 “credit monitoring” damages range from under \$100 to over \$1000. *See* Ex. D,  
6 Levine Tr. 196; Ex. E, Archibeque Tr. 34; Ex. K, Bailey Tr. 138-40; Ex. B,  
7 Johnson Rep. ¶ 25 & Ex. 2. Given that variation, it is impossible to see how costs  
8 incurred by these eight Plaintiffs are “representative” of any costs incurred by  
9 thousands of other classmembers—as to whom there is *no* evidence in the record—  
10 or how Fishkind’s “model” can prove injury or damages on a classwide basis,  
11 much less *any* injury or damages whatsoever to an absent putative classmember.  
12 Ex. L, Fishkind Tr. 121-23; Ex. B, Johnson Rep. ¶¶ 68-75.

13 **b) Individualized issues predominate with respect to**  
14 **prophylactic costs**


15 As the Court has explained, to determine whether prophylactic costs are  
16 reasonable and necessary in any given case, the factfinder must consider several  
17 plaintiff-specific factors. *See Potter*, 6 Cal. 4th at 1009 (listing factors). That  
18 multi-factor test is unsuited for class treatment, as courts have routinely recognized  
19 in denying certification of monitoring claims. *See, e.g., In re St. Jude Med., Inc.*,  
20 425 F.3d 1116, 1122 (8th Cir. 2005) (class certification precluded because “each  
21 plaintiff’s need (or lack of need) for medical monitoring is highly individualized,”  
22 collecting cases); *Lockheed Martin v. Sup. Ct.*, 29 Cal. 4th 1096, 1108-11 (2003)  
23 (applying *Potter*, denying certification).

24 Start with the third *Potter* factor: “the relative increase in the risk of identity  
25 theft when compared to (a) Plaintiffs’ chances of identity theft had the data breach  
26 not occurred, and (b) the chances of the public at large being subject to identity  
27 theft.” Although Plaintiffs’ expert confidently asserted in his report that “[e]very  
28 victim of the SPE data breach faces the same risk of harms over a very long time

1 horizon” (Ponemon Rep. ¶ 37), that is incorrect and irrelevant. It is incorrect  
2 because most people whose PII is exposed in a data breach will likely never  
3 experience any misuse; even among those who do, most do not suffer any actual  
4 injury because their financial institutions reimburse them for any fraudulent  
5 activity. Ex. A, Turner Rep. ¶¶ 24, 36, 82. It is also irrelevant because Ponemon  
6 admitted at his deposition that he could not opine on the amount by which any  
7 classmember’s risk of identity fraud had increased as a result of the cyberattack.  
8 Ex. M, Ponemon Tr. 147-49 (“What we don’t know is the rate of increase. Is it a 1  
9 percent chance, a 10 percent, that is not known to me as a researcher or to anyone  
10 else who does research in this area, to the best of my knowledge.”). *Cf.*  
11 *Stollenwerk v. Tri-West Healthcare*, 2005 WL 2465906, at \*5 (D. Ariz. Sept. 6,  
12 2005) (finding “no evidence ... that credit monitoring will reduce the risk of  
13 identity fraud to the necessary degree” because plaintiffs’ expert “fails to quantify  
14 the reduction of risk in objective terms”), *aff’d in relevant part*, 254 F. App’x 664,  
15 665-67 (9th Cir. 2007). Ponemon also conceded that the risk of identity theft  
16 would vary among the classmembers after the cyberattack, and that for some the  
17 risk of identity theft could even *decrease*. Ex. M, Ponemon Tr. 133-35, 148-49,  
18 153-54. Finally, as to Ponemon’s assertion that any risks would persist for a long  
19 time, he admitted that he is in fact not aware of any studies supporting that  
20 assertion—“that research has never been done”—but rather, “[i]t’s like one of  
21 those things that you hear. You just assume it to be true.” *Id.* at 202-03, 210.

22       Regardless, Ponemon’s report fails to compare the alleged increased risk of  
23 identity theft with each classmember’s “chances of identity theft had the data  
24 breach not occurred.” Even under the *Potter* analogy, monitoring would be  
25 available only to those whose risk has been appreciably increased by the  
26 cyberattack. Determining whether an individual classmember has experienced any  
27 “relative increase” in risk—and if so, how much—requires examination of each  
28 classmember’s baseline risk, absent the cyberattack. That risk varies widely and

1 depends on a host of facts specific to each individual. Again, as Plaintiffs  
2 themselves confirm, some classmembers are likely already at great risk of  
3 “familiar fraud”—fraud by someone to whom they directly provided PII. *See*

4   
5 continue to be) victims of other data breaches. *See supra* at 4. Still more  
6 classmembers will have voluntarily shared their PII online. *Id.* For these and other  
7 classmembers, the risk of identity theft absent the cyberattack was already  
8 relatively high; if the attack increased that risk at all, any increase was minor. Ex.  
9 A, Turner Rep. ¶¶ 69-70. As to each of them, SPE is entitled to and will defend  
10 against any claim for costs of monitoring on that ground.

11 The “significance and extent of the compromise to Plaintiffs’ PII”—the first  
12 *Potter* factor—will also vary across the class. For some, the released information  
13 may have been significant. For others, however, it may have been out of date, or  
14 not the kind of information that renders an individual susceptible to identity theft,  
15 and thus of little or no value to thieves. Ex. A, Turner Rep. ¶¶ 45, 57-64. Again,  
16 Plaintiffs’ own experiences prove the point. Forster suspects that his bank account  
17 information, driver’s license, and resident alien card were disclosed, but  
18 acknowledges such information is “worthless” or “useless” because the bank  
19 account is closed and the cards have both expired. *See* Ex. H, Forster Tr. 34-38.  
20 And Mathis believes that her former home address was disclosed, but  
21 acknowledges that the former address is not associated with any of her current  
22 financial accounts. Ex. G, Mathis Tr. 53, 383; Ex. A, Turner Rep. ¶ 57.

23 Plaintiffs ignore this variation across the class. They say *nothing* about  
24 whether putative classmembers are united by disclosure of some common PII  
25 elements. Pls.’ Mem. 2 (disclosed PII included, “among other things,” eleven  
26 separate categories of information, none of which they say is common to all  
27 classmembers). Instead, they insist that the disclosure of an SSN, standing alone,  
28 suffices to expose a classmember to a sufficient risk of future harm to render future

1 monitoring costs both reasonable and necessary. Ponemon Rep. ¶¶ 25, 31. But  
2 Plaintiffs cannot even show that this theory holds with respect to the eight of them,  
3 as they offer no evidence that Mathis’s SSN was disclosed. *See supra* at 3. In any  
4 event, as Turner shows and Plaintiffs have admitted, SSNs are regularly disclosed  
5 in a wide variety of contexts, including many data breaches. *See Ex. A, Turner*  
6 *Rep. ¶¶ 20-21; see also, e.g., Ex. E, Archibeque Tr. 97-99, 114; Ex. H, Forster Tr.*  
7 *204-06; Ex. G, Mathis Tr. 131-32.* The “significance” of having an SSN disclosed  
8 in the SPE cyberattack thus varies from person to person. Further, an SSN  
9 standing alone is rarely enough to carry out identity theft. *Ex. A, Turner Rep.*  
10 *¶¶ 45-49.* Other PII is generally necessary, and there is material variation across  
11 the class as to whether any such additional information, sufficient to expose a  
12 classmember to an increased risk of identity theft, was disclosed in the cyberattack.

13 In short, no class can be certified to recover prophylactic costs because  
14 individualized questions of reasonableness and necessity predominate. Even if all  
15 classmembers had significant PII disclosed—and they did not—the inquiry into  
16 whether particular prophylactic measures were reasonable or necessary for each of  
17 them would necessarily devolve into thousands of mini-trials.

## 18 2. Differences In State Law Preclude Certification

19 Finally, Plaintiffs say their negligence class should be certified on a medical-  
20 monitoring theory, notwithstanding differences in state law, because California has  
21 an interest in applying its law to SPE. Plaintiffs ignore, however, that there is  
22 broad disagreement among the States as to the propriety of recovery for monitoring  
23 expenses. Certification of a nationwide class would fail Rule 23’s predominance  
24 requirement because of differences in state law concerning the availability of  
25 prophylactic damages. *See In re Rezulin Litig.*, 210 F.R.D. 61, 71 (S.D.N.Y. 2002).

26 Many States reject tort liability for medical monitoring claims absent actual  
27 physical injury, emphasizing that it “departs drastically from ... traditional notions  
28 of a valid negligence claim.” *Henry v. Dow Chem. Co.*, 701 N.W. 2d 684, 694

1 (Mich. 2005); *see also, e.g., Wood v. Wyeth-Ayerst Labs.*, 82 S.W. 3d 849, 856-59  
2 (Ky. 2002). SPE is not aware of any State that has extended the theory to cover  
3 monitoring costs in a data-breach case. *Cf. Stollenwerk*, 254 F. App'x at 668-69  
4 (declining to certify question whether Arizona recognizes monitoring claim); *Ruiz*  
5 *v. Gap, Inc.*, 622 F. Supp. 2d 908, 914 (N.D. Cal. 2009) (“doubt[ing] a California  
6 court would view” “lost-data cases as analogous to medical monitoring cases”).

7 As the Ninth Circuit has recognized, “every state has an interest in having its  
8 law applied to its resident claimants.” *Mazza v. Am. Honda Motor Co.*, 666 F.3d  
9 581, 591-92 (9th Cir. 2012). The States where non-California classmembers reside  
10 thus have a strong interest in enforcing their considered policy judgments as to the  
11 recoverability of monitoring costs. States that reject medical monitoring cite the  
12 risk that “[l]itigation of these preinjury claims could drain resources needed to  
13 compensate those with manifest physical injuries and a more immediate need for  
14 medical care,” *Henry*, 701 N.W.2d at 694, and note that claim preclusion would  
15 prevent classmembers from bringing subsequent claims if they developed an injury  
16 or illness in the future, *Wood*, 82 S.W.3d at 858. This emphatic rejection by many  
17 States of recovery for monitoring refutes Plaintiffs’ suggestion (at 18-19) that  
18 “applying California law to nonresident plaintiffs will vindicate foreign states’  
19 interests in compensating their residents.” To the contrary, those States have made  
20 the judgment that their residents ought *not* be compensated for these speculative  
21 risks of future injury. Unlike the general choice-of-law cases Plaintiffs cite (at  
22 18)—none of which has anything to do with monitoring—the rationale for this  
23 judgment is not protection of in-state business defendants from liability, but rather  
24 preservation of the opportunity for resident-plaintiffs who sustain actual injuries in  
25 the future to meaningfully recover.

## 26 **II. NO CLASS CAN BE CERTIFIED ON THE CMIA CLAIM**

27 To certify a class on their CMIA claim, Plaintiffs must demonstrate they can  
28 prove through generalized evidence that, among other things, all classmembers had

1 “medical information” disclosed in the cyberattack. “Medical information” is a  
2 defined statutory term, limited to “any individually identifiable information ... in  
3 *possession of or derived from*” certain healthcare providers enumerated in the  
4 statute. Cal. Civ. Code § 56.05(j) (emphasis added). Plaintiffs make absolutely no  
5 effort to demonstrate they can prove this element on a classwide basis.

6 To start, because no *Plaintiff* can assert a CMIA claim, none can satisfy the  
7 typicality requirement. Plaintiffs alleged in their complaint that they “believe[d]”  
8 their medical information was disclosed (*see, e.g.*, Am. Compl. ¶ 122 (Shapiro)),  
9 but allegations do not suffice for class certification, and in any event that “belie[f]”  
10 has proven to be false (*see, e.g.*, Ex. F, Shapiro Tr. 21-24 (Shapiro’s own search of  
11 released PII revealed no medical information)). SPE has produced documents  
12 sufficient to show whether any even arguable medical information relating to  
13 Plaintiffs was disclosed. Plaintiffs have pointed to none, and there is none. Absent  
14 a Plaintiff with a CMIA claim, no class can be certified. *See Flores v. CVS Pharm.,*  
15 *Inc.*, 2010 WL 3656807, at \*7-8 (C.D. Cal. Sept. 7, 2010) (plaintiff “cannot be  
16 deemed ‘typical’ of all class members” when she “has no claim”).

17 Further, Plaintiffs never say—nor could they—that *all* members of their  
18 proposed class can assert a CMIA claim, since only a fraction of those individuals  
19 had any health-related information disclosed in the cyberattack. Because Plaintiffs’  
20 class definition includes many thousands of putative classmembers who have no  
21 CMIA claim, the class they propose cannot be certified. *Moore*, 2015 WL  
22 4638293, at \*8 (“class cannot be certified” where it “is so broad that it sweeps  
23 within it persons who could not have been injured by the defendant’s conduct”).

24 Plaintiffs may say in reply that the Court ought to certify a CMIA subclass.  
25 But Plaintiffs’ typicality failure would doom the subclass too; there is no  
26 representative. Any subclass also would fail the predominance requirement.  
27 Plaintiffs neither plead nor offer proof that SPE is a covered healthcare provider—  
28 nor could they. Their only theory accordingly must be that certain classmembers’



1 medical information was “derived from” a healthcare provider—*i.e.*, an entity  
2 other than SPE. Even if there were a subclass representative, Plaintiffs offer no  
3 explanation of how they could prove through generalized evidence applicable to  
4 the subclass as a whole that subclassmembers’ disclosed health information was  
5 “derived from” a covered healthcare provider, and thus constitutes “medical  
6 information” within the meaning of the statute. *Cf. Farmer v. Phillips Agency, Inc.*,  
7 285 F.R.D. 688, 703 (N.D. Ga. 2012) (denying class certification of FCRA claim  
8 because “court would need to determine the source of each piece of adverse  
9 information in a consumer’s report and then evaluate the quality of that source”).

### 10 **III. NO CLASS CAN BE CERTIFIED ON THE UCL CLAIM**

11 The Court allowed Plaintiffs’ UCL cause of action to go forward to the  
12 extent that “predicate claims that form the basis for” the claim survived. 2015 WL  
13 3916744, at \*8. Just as Plaintiffs’ negligence and CMIA claims cannot be  
14 certified, “it follows that [their] UCL [claim under the unlawful prong] also is not  
15 suitable for classwide treatment.” *Faulk v. Sears Roebuck & Co.*, 2013 WL  
16 1703378, at \*10 (N.D. Cal. Apr. 19, 2013). Plaintiffs nonetheless insist that they  
17 can also pursue their UCL claim under the “fraudulent” and “unfair” prongs. The  
18 Court did not say those claims could proceed, and they too cannot be certified.

19 *Fraudulent prong.* Under the UCL, named “plaintiffs must plead and prove  
20 actual reliance” on the challenged misrepresentations and omissions. *In re*  
21 *Tobacco II Cases*, 46 Cal. 4th 298, 328 (2009); *see* Pls.’ Mem. 13 (“named  
22 plaintiffs [must] demonstrate injury and causation”). Here, all Plaintiffs began  
23 work at SPE before 2005—that is, well before the misrepresentations they allege,  
24 and before they allege the company was made aware of purported security  
25 deficiencies that would have rendered subsequent statements incomplete. *See* Am.  
26 Compl. ¶¶ 43, 77, 83, 89, 95, 99, 105, 111, 118. Because no Plaintiff was exposed  
27 to the misrepresentations or omissions they allege, they necessarily could not have  
28 *relied* on them, and thus cannot represent the class. *See Quezada v. Loan Ctr. of*

1 *Cal., Inc.*, 2009 WL 5113506, at \*7 (E.D. Cal. Dec. 18, 2009).<sup>8</sup>

2 Even if there were a typical class representative, individualized issues would  
3 predominate. Plaintiffs must show they can prove, on a classwide basis, that  
4 classmembers “were actually exposed to the business practices at issue.” *Berger v.*  
5 *Home Depot USA, Inc.*, 741 F.3d 1061, 1068 (9th Cir. 2014). They default entirely.  
6 The only specific misrepresentation they allege is a statement made in reference to  
7 a different Sony company, well after Plaintiffs (and much of the class) began  
8 working for SPE—not an ““extensive and longterm fraudulent advertising  
9 campaign.”” *Id.*; see Am. Compl. ¶ 211. They say even less about SPE’s alleged  
10 omissions. No common proof can establish a classwide violation of the UCL’s  
11 fraudulent prong. See *Berger*, 741 F.3d at 1069; see also *Mazza*, 666 F.3d at 596.

12 *Unfair prong.* To prevail here, Plaintiffs must show that SPE’s conduct  
13 caused injuries to them and classmembers. *In re Firearm Cases*, 24 Cal. Rptr. 3d  
14 659, 674 (App. 2005). Because the injuries alleged here are identical to those  
15 alleged under Plaintiffs’ negligence claim, the same individualized questions will  
16 predominate here. See *supra* Section I.B; *Campion v. Old Republic Home*  
17 *Protection Co.*, 272 F.R.D. 517, 533 (S.D. Cal. 2011).

18 Individualized issues would also predominate regarding litigation of the  
19 balancing test under the unfair prong, under which courts “must weigh ‘the utility

20 \_\_\_\_\_  
21 <sup>8</sup> Further to the point, no Plaintiff testified that SPE’s data security played a  
22 role in their decision to accept employment and provide their PII to SPE. See Ex.  
23 E, Archibeque Tr. 86-87; Ex. D, Levine Tr. 125-27; Ex. G, Mathis Tr. 349-51; Ex.  
24 I, Corona Tr. 290; Ex. J, Springer Tr. 42, 45; Ex. H, Forster Tr. 173, 175. At most,  
25 Bailey testified that she “expected” her personal information would be protected  
26 when she started work in 1991 (Ex. K, Bailey Tr. 44-45), and Shapiro testified that  
27 he inquired “how [his PII] was going to be used and whether it was required,” and  
28 was told “the purposes of what it was used for, for example, for beneficiaries or  
emergency contact information or other similar purposes” (Ex. F, Shapiro Tr. 119).  
None of this relates to any alleged misrepresentation or omission, and none of this  
shows reliance. Because no Plaintiff even arguably relied on the alleged  
misrepresentations or omissions, no class can be certified.



1 of the defendant’s conduct against the gravity of the harm to the alleged victim.”  
2 *Davis v. HSBC Bank, N.A.*, 691 F.3d 1152, 1169 (9th Cir. 2012). As discussed  
3 above (Section I.B), the harm (if any) to each classmember will vary widely;  
4 weighing the utility of SPE’s information security practices against the alleged  
5 harm to each classmember cannot be performed on a classwide basis. *See*  
6 *Herskowitz v. Apple, Inc.*, 301 F.R.D. 460, 476 (N.D. Cal. 2014).

7 One final point bears mention. In addition to affirmative injunctive relief “in  
8 the form of changes to SPE’s data security practices,” Plaintiffs seek an injunction  
9 under the UCL requiring “the provision of identity theft protection, monitoring and  
10 recovery services.” Pls.’ Mem. 14. Plaintiffs offer no authority for that request,  
11 nor could they. Rather, because “Plaintiffs’ proposed injunction is practically  
12 indistinguishable from an order that [SPE] pay Plaintiffs money,” it is  
13 impermissible. *Herskowitz*, 301 F.R.D. at 482 (collecting cases). Further, their  
14 request for an order paying them what are essentially damages is doubly  
15 impermissible under the UCL, which does not provide for damages at all. *De La*  
16 *Torre v. CashCall, Inc.*, 56 F. Supp. 3d 1105, 1108 (N.D. Cal. 2014).

#### 17 **IV. NO CLASS CAN BE CERTIFIED ON DECLARATORY JUDGMENT**

18 Plaintiffs’ claim for declaratory relief is based exclusively on their  
19 negligence claim and their now-dismissed contract claim. *See* Am. Compl.  
20 ¶ 220. As the Ninth Circuit has explained, where the need for individualized  
21 inquiry would defeat “certification of a potential nationwide class” on a plaintiff’s  
22 underlying substantive claim, “then the same predominance analysis applies with  
23 equal force to preclude [plaintiff’s Declaratory Judgment Act] claim.” *Lozano v.*  
24 *AT&T Wireless Servs., Inc.*, 504 F.3d 718, 729 (9th Cir. 2007). Because no class  
25 can be certified on Plaintiffs’ predicate negligence claim, it follows that no class  
26 can be certified here.

#### 27 **CONCLUSION**

28 Plaintiffs’ Motion for Class Certification should be denied.

1 Dated: August 11, 2015

Respectfully submitted,

2 By: /s/ William F. Lee  
3 William F. Lee

4 WILMER CUTLER PICKERING  
5 HALE AND DORR LLP

6 Attorneys for Defendant

7 SONY PICTURES ENTERTAINMENT INC.  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28