

United States District Court
For the Northern District of California

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

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

)	Case No.: 13-CV-05226-LHK
)	
IN RE ADOBE SYSTEMS, INC. PRIVACY)	ORDER GRANTING IN PART AND
LITIGATION)	DENYING IN PART DEFENDANT
)	ADOBE SYSTEMS INC.'S MOTION TO
)	DISMISS

In this consolidated litigation, Plaintiffs Christian Duke (“Duke”), Joseph Kar (“Kar”), Christina Halpain (“Halpain”), Jacob McHenry (“McHenry”), Anne McGlynn (“McGlynn”), and Marcel Page (“Page”), individually and on behalf of those similarly situated (collectively, “Plaintiffs”) bring claims against Defendant Adobe Systems, Inc. (“Adobe”) arising out of an intrusion into Adobe’s computer network in 2013 and the resulting data breach. Consol. Compl. (“Compl.”) ECF No. 39. Pending before the Court is Adobe’s Motion to Dismiss, in which Adobe seeks dismissal of all of Plaintiffs’ claims. (“Mot.”) ECF No. 45. Plaintiffs have filed an Opposition, (“Opp’n”) ECF No. 47, and Adobe has filed a Reply, (“Reply”) ECF No. 50. Having considered the submissions of the parties and the relevant law, the Court hereby GRANTS IN PART and DENIES IN PART Adobe’s Motion to Dismiss.

1 **I. BACKGROUND**

2 **A. Factual Allegations**

3 Except where indicated, the facts in this section are taken from Plaintiffs' Complaint and
4 accepted as true for the purposes of this Motion.

5 **1. Adobe's Products and Services**

6 Adobe is a multinational software company that sells and licenses printing, publishing,
7 multimedia, and graphics software. Compl. ¶ 17. Adobe sells a wide range of products, including
8 Photoshop (a widely-used digital imaging program) and ColdFusion (used by web developers to
9 build websites and Internet applications). *Id.* ¶ 19. Adobe's products and services are available in
10 two forms. Some Adobe software, such as ColdFusion, is sold through licenses, where customers
11 pay a single licensing fee to use the software. *Id.* Other Adobe products are available through
12 Adobe's subscription-based "Creative Cloud," where customers pay a monthly fee to use Adobe's
13 products and services. *Id.*

14 Adobe collects a variety of customer information. Customers of licensed-based products
15 must register their products, which requires customers to provide Adobe with their e-mail
16 addresses and create a username and password for Adobe's website. *Id.* Some of these customers
17 purchased their licenses online from Adobe directly, and thus also provided Adobe with their credit
18 card numbers and expiration dates, as well as other billing information. *E.g., id.* ¶¶ 19, 78, 96.
19 Creative Cloud customers are required to keep an active credit card on file with Adobe, which is
20 charged automatically according to the customer's subscription plan. *Id.* ¶ 19. In addition, some
21 Creative Cloud customers store their files and work products in Adobe's "cloud." *E.g., id.* ¶ 84. As
22 a result of the popularity of Adobe's products, Adobe has collected personal information in the
23 form of names, e-mail and mailing addresses, telephone numbers, passwords, credit card numbers
24 and expiration dates from millions of customers. *Id.* ¶¶ 22, 50-55.

25 All customers of Adobe products, including Creative Cloud subscribers, are required to
26 accept Adobe's End-User License Agreements ("EULA") or General Terms of Use. *Id.* ¶ 29. Both
27 incorporate Adobe's Privacy Policy, which provides in relevant part: "[Adobe] provide[s]
28

1 reasonable administrative, technical, and physical security controls to protect your information.
2 However, despite our efforts, no security controls are 100% effective and Adobe cannot ensure or
3 warrant the security of your personal information.” (“Agreement”) ECF No. 46-2 at 4. Adobe’s
4 Safe Harbor Privacy Policy, which supplements Adobe’s Privacy Policy, similarly provides that
5 “Adobe . . . uses reasonable physical, electronic, and administrative safeguards to protect your
6 personal information from loss; misuse; or unauthorized access, disclosure, alteration, or
7 destruction.” Compl. ¶ 32. Adobe makes similar representations regarding its security practices on
8 its websites. *Id.* ¶¶ 33-39.

9 2. **The 2013 Data Breach**

10 In July 2013, hackers gained unauthorized access to Adobe’s servers. *Id.* ¶ 48. The hackers
11 spent several weeks inside Adobe’s network without being detected. *Id.* By August 2013, the
12 hackers reached the databases containing customers’ personal information, as well as the source
13 code repositories for Adobe products. *Id.* The hackers then spent up to several weeks removing
14 customer data and Adobe source code from Adobe’s network, all while remaining undetected. *Id.*
15 The data breach did not come to light until September, when independent security researchers
16 discovered stolen Adobe source code on the Internet. *Id.* ¶ 49. Adobe announced the data breach on
17 October 3, 2013. *Id.* ¶ 50. Adobe announced that the hackers accessed the personal information of
18 at least 38 million customers, including names, login IDs, passwords, credit and debit card
19 numbers, expiration dates, and mailing and e-mail addresses. *Id.* ¶¶ 50-52. Adobe confirmed that
20 the hackers copied the source code for a number of its products, including ColdFusion. *Id.* ¶ 53.
21 Adobe subsequently disclosed that the hackers were able to use Adobe’s systems to decrypt
22 customers’ credit card numbers, which had been stored in an encrypted form. *Id.* ¶ 57. The Court
23 will refer to this sequence of events as the “2013 data breach.”

24 Following the 2013 data breach, researchers concluded that Adobe’s security practices were
25 deeply flawed and did not conform to industry standards. *Id.* ¶ 59. For example, though customers’
26 passwords had been stored in encrypted form, independent security researchers analyzing the
27 stolen passwords discovered that Adobe’s encryption scheme was poorly implemented, such that
28

1 the researchers were able to decrypt a substantial portion of the stolen passwords in short order. *Id.*
2 ¶ 63. Adobe similarly failed to employ intrusion detection systems, properly segment its network,
3 or implement user or network level system controls. *Id.* ¶ 62. As a result of the 2013 data breach,
4 Adobe offered its customers one year of free credit monitoring services and advised customers to
5 monitor their accounts and credit reports for fraud and theft. *Id.* ¶¶ 54, 56.

6 **3. The Plaintiffs**

7 Plaintiffs are customers of Adobe licensed products or Creative Cloud subscribers who
8 provided Adobe with their personal information. Plaintiffs Kar and Page purchased licensed
9 products directly from Adobe and provided Adobe with their names, email addresses, credit card
10 numbers, other billing information, and other personal information. *Id.* ¶¶ 77-78, 95-96. Plaintiff
11 McHenry purchased an Adobe licensed product, and provided Adobe with a username and
12 password. *Id.* ¶¶ 98-99. Plaintiffs Duke, Halpain, and McGlynn subscribed to Adobe's products,
13 and provided Adobe with their names, email addresses, credit card numbers, other billing
14 information, and other personal information. *Id.* ¶¶ 74-75, 83-84, 90. Plaintiffs Duke, Kar, Halpain,
15 and McGlynn are California citizens and residents. *Id.* ¶¶ 10-12, 14. Adobe informed all Plaintiffs
16 that their personal information had been compromised as a result of the 2013 data breach. *Id.* ¶¶ 76,
17 80, 85, 92, 97, 100. Following the 2013 data breach, Plaintiffs Kar and Halpain purchased
18 additional credit monitoring services. *Id.* ¶¶ 81, 86.

19 **B. Procedural History**

20 The seven cases underlying this consolidated action were filed in this Court between
21 November 2013 and January 2014. *See* ECF No. 1; Case No. 13-CV-5611, ECF No. 1; Case No.
22 13-CV-5596, ECF No. 1; Case No. 13-CV-5930, ECF No. 1; Case No. 14-CV-14, ECF No. 1;
23 Case No. 14-CV-30, ECF No. 1; Case No. 14-CV-157, ECF No. 1. The Court related the
24 individual cases in December 2013 and January 2014, ECF Nos. 19, 22, 26,¹ and consolidated them
25 on March 13, 2014, ECF No. 34. Plaintiffs filed their Consolidated Complaint on April 4, 2014.
26 ECF No. 39. Adobe filed its Motion to Dismiss on May 21, 2014, ECF No. 45, with an
27

28 ¹ Unless otherwise noted, all remaining ECF citations refer to Case Number 13-CV-5226.

1 accompanying Request for Judicial Notice, (“Def. May 21 RJN”) ECF No. 46. Plaintiffs filed their
 2 Opposition on June 11, 2014, ECF No. 47, with an accompanying Request for Judicial Notice,
 3 (“Pl. RJN”) ECF No. 48. Adobe filed its Reply on July 2, 2014, ECF No. 50, along with a second
 4 Request for Judicial Notice, (“Def. July 2 RJN”) ECF No. 51.²

5 **II. LEGAL STANDARDS**

6 **A. Rule 12(b)(1)**

7 A defendant may move to dismiss an action for lack of subject matter jurisdiction pursuant
 8 to Federal Rule of Civil Procedure 12(b)(1). A motion to dismiss for lack of subject matter
 9 jurisdiction will be granted if the complaint on its face fails to allege facts sufficient to establish
 10 subject matter jurisdiction. *See Savage v. Glendale Union High Sch.*, 343 F.3d 1036, 1039 n.2 (9th
 11 Cir. 2003). If the plaintiff lacks standing under Article III of the U.S. Constitution, then the court
 12 lacks subject matter jurisdiction, and the case must be dismissed. *See Steel Co. v. Citizens for a*
 13 *Better Env’t*, 523 U.S. 83, 101-02 (1998). In considering a Rule 12(b)(1) motion, the Court “is not

14 ² Although a district court generally may not consider any material beyond the pleadings in
 15 deciding a Rule 12(b)(6) motion, the Court may take judicial notice of documents referenced in the
 16 complaint, as well as matters in the public record, without converting a motion to dismiss into one
 17 for summary judgment. *See Lee v. City of L.A.*, 250 F.3d 668, 688-89 (9th Cir. 2001). A matter
 18 may be judicially noticed if it is either “generally known within the trial court’s territorial
 19 jurisdiction,” or “can be accurately and readily determined from sources whose accuracy cannot
 20 reasonably be questioned.” Fed. R. Evid. 201(b).

21 Here, Adobe requests that the Court take judicial notice of the transcript of the case
 22 management conference hearing held before this Court on March 13, 2014. Def. May 21 RJN Ex.
 23 A. This transcript is an appropriate subject for judicial notice, as it is a matter of public record.
 24 Adobe also requests that the Court take judicial notice of Adobe’s Privacy Policies of May 7, 2012
 25 and December 20, 2013, *id.* Exs. B, C; Adobe’s General Terms of Use, *id.* Ex. D; and the
 26 subscription terms for Adobe’s Creative Cloud, *id.* Ex. E. These documents are referenced and
 27 quoted in the Complaint, *e.g.*, Compl. ¶¶ 5, 29, 30-32, 84, 91, 99, 119-120, 129, and the Court may
 28 therefore take judicial notice of these documents under the doctrine of incorporation by reference.
See, e.g., Knievel v. ESPN, 393 F.3d 1068, 1076 (9th Cir. 2005) (district court may consider
 “documents whose contents are alleged in a complaint and whose authenticity no party questions,
 but which are not physically attached to the [plaintiff’s] pleading” (alteration in original) (internal
 quotation marks omitted)). Finally, Adobe requests that the Court take judicial notice of three
 newspaper articles discussing Adobe’s security problems. Def. July 2 RJN Exs. A, B, C. The Court
 may take judicial notice of the existence of these reports as indication of what was in the public
 realm, but not for the veracity of any arguments or facts contained within. *See Von Saher v. Norton*
Simon Museum of Art at Pasadena, 592 F.3d. 954, 960 (9th Cir. 2010). Accordingly, the Court
 GRANTS Adobe’s Requests for Judicial Notice dated May 21, 2014 and July 2, 2014.

Plaintiffs request that the Court take judicial notice of one of Adobe’s End User License
 Agreements (“EULA”). Pl. RJN Ex. A. The EULA is referenced in the Complaint, *see, e.g.*,
 Compl. ¶¶ 29-32, 41, 105, and is publicly available on Adobe’s website. Accordingly, the Court
 GRANTS Plaintiffs’ Request for Judicial Notice. *See Knievel*, 393 F.3d at 1076.

1 restricted to the face of the pleadings, but may review any evidence, such as affidavits and
2 testimony, to resolve factual disputes concerning the existence of jurisdiction.” *McCarthy v. United*
3 *States*, 850 F.2d 558, 560 (9th Cir. 1988). Once a party has moved to dismiss for lack of subject
4 matter jurisdiction under Rule 12(b)(1), the opposing party bears the burden of establishing the
5 court’s jurisdiction, *see Chandler v. State Farm Mut. Auto. Ins. Co.*, 598 F.3d 1115, 1122 (9th Cir.
6 2010), by putting forth “the manner and degree of evidence required” by whatever stage of the
7 litigation the case has reached, *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992); *see also*
8 *Barnum Timber Co. v. Env’tl. Prot. Agency*, 633 F.3d 894, 899 (9th Cir. 2011) (at the motion to
9 dismiss stage, Article III standing is adequately demonstrated through allegations of “specific facts
10 plausibly explaining” why the standing requirements are met).

11 **B. Rule 8(a)**

12 Rule 8(a)(2) of the Federal Rules of Civil Procedure requires a complaint to include “a
13 short and plain statement of the claim showing that the pleader is entitled to relief.” A complaint
14 that fails to meet this standard may be dismissed pursuant to Federal Rule of Civil Procedure
15 12(b)(6). The Supreme Court has held that Rule 8(a) requires a plaintiff to plead “enough facts to
16 state a claim to relief that is plausible on its face.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570
17 (2007). “A claim has facial plausibility when the plaintiff pleads factual content that allows the
18 court to draw the reasonable inference that the defendant is liable for the misconduct alleged.”
19 *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). “The plausibility standard is not akin to a probability
20 requirement, but it asks for more than a sheer possibility that a defendant has acted unlawfully.” *Id.*
21 (internal quotation marks omitted). For purposes of ruling on a Rule 12(b)(6) motion, a court
22 “accept[s] factual allegations in the complaint as true and construe[s] the pleadings in the light
23 most favorable to the nonmoving party.” *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d
24 1025, 1031 (9th Cir. 2008).

25 However, the Court need not accept as true allegations contradicted by judicially noticeable
26 facts, *Shwarz v. United States*, 234 F.3d 428, 435 (9th Cir. 2000), and the “[C]ourt may look
27 beyond the plaintiff’s complaint to matters of public record” without converting the Rule 12(b)(6)
28

1 motion into one for summary judgment, *Shaw v. Hahn*, 56 F.3d 1128, 1129 n.1 (9th Cir. 1995).
2 Nor is the Court required to “assume the truth of legal conclusions merely because they are cast in
3 the form of factual allegations.” *Fayer v. Vaughn*, 649 F.3d 1061, 1064 (9th Cir. 2011) (per
4 curiam) (quoting *W. Mining Council v. Watt*, 643 F.2d 618, 624 (9th Cir. 1981)). Mere “conclusory
5 allegations of law and unwarranted inferences are insufficient to defeat a motion to dismiss.”
6 *Adams v. Johnson*, 355 F.3d 1179, 1183 (9th Cir. 2004); *accord Iqbal*, 556 U.S. at 678.
7 Furthermore, plaintiffs may plead themselves out of court if they “plead facts which establish that
8 [they] cannot prevail on [their] . . . claim.” *Weisbuch v. Cnty. of L.A.*, 119 F.3d 778, 783 n.1 (9th
9 Cir. 1997) (internal quotation marks and citation omitted).

10 C. Rule 9(b)

11 Claims sounding in fraud or mistake are subject to the heightened pleading requirements of
12 Federal Rule of Civil Procedure 9(b), which requires that a plaintiff alleging fraud “must state with
13 particularity the circumstances constituting fraud.” Fed. R. Civ. P. 9(b); *see Kearns v. Ford Motor*
14 *Co.*, 567 F.3d 1120, 1124 (9th Cir. 2009). To satisfy Rule 9(b)’s heightened standard, the
15 allegations must be “specific enough to give defendants notice of the particular misconduct which
16 is alleged to constitute the fraud charged so that they can defend against the charge and not just
17 deny that they have done anything wrong.” *Semegen v. Weidner*, 780 F.2d 727, 731 (9th Cir.
18 1985). Thus, claims sounding in fraud must allege “an account of the time, place, and specific
19 content of the false representations as well as the identities of the parties to the misrepresentations.”
20 *Swartz v. KPMG LLP*, 476 F.3d 756, 764 (9th Cir. 2007) (per curiam) (internal quotation marks
21 omitted). “The plaintiff must set forth what is false or misleading about a statement, and why it is
22 false.” *In re Glenfed, Inc. Sec. Litig.*, 42 F.3d 1541, 1548 (9th Cir. 1994) (en banc), *superseded by*
23 *statute on other grounds as stated in Ronconi v. Larkin*, 253 F.3d 423, 429 n.6 (9th Cir. 2001).

24 D. Leave to Amend

25 If the Court determines that the complaint should be dismissed, it must then decide whether
26 to grant leave to amend. Under Rule 15(a) of the Federal Rules of Civil Procedure, leave to amend
27 “should be freely granted when justice so requires,” bearing in mind that “the underlying purpose
28

1 of Rule 15 . . . [is] to facilitate decision on the merits, rather than on the pleadings or
 2 technicalities.” *Lopez v. Smith*, 203 F.3d 1122, 1127 (9th Cir. 2000) (en banc) (internal quotation
 3 marks omitted). Nonetheless, a court “may exercise its discretion to deny leave to amend due to
 4 ‘undue delay, bad faith or dilatory motive on part of the movant, repeated failure to cure
 5 deficiencies by amendments previously allowed, undue prejudice to the opposing party . . . , [and]
 6 futility of amendment.’” *Carvalho v. Equifax Info. Servs., LLC*, 629 F.3d 876, 892-93 (9th Cir.
 7 2010) (alterations in original) (quoting *Foman v. Davis*, 371 U.S. 178, 182 (1962)).

8 **III. DISCUSSION**

9 Plaintiffs assert four causes of action in their Complaint. Adobe seeks dismissal of all four
 10 claims. The Court will address each claim and Adobe’s corresponding objections in turn.

11 **A. Customer Records Act Claim**

12 Plaintiffs’ first cause of action is for injunctive relief on behalf of the California Plaintiffs
 13 for violations of Sections 1798.81.5 and 1798.82 of the California Civil Code (“CRA”).³ The CRA
 14 provides in relevant part that:

15 A business that owns or licenses personal information about a California resident
 16 shall implement and maintain reasonable security procedures and practices
 17 appropriate to the nature of the information, to protect the personal information
 18 from unauthorized access, destruction, use, modification, or disclosure.

19 Cal. Civ. Code § 1798.81.5(b). Section 1798.82, for its part, requires businesses to “disclose any
 20 breach of the security of the system following discovery or notification of the breach . . . in the
 21 most expedient time possible and without unreasonable delay.” Cal. Civ. Code § 1798.82(a).

22 Plaintiffs allege that Adobe did not and does not maintain “reasonable security practices” to protect
 23 customer data, in violation of Section 1798.81.5 of the CRA, and did not promptly notify

24 _____
 25 ³ Adobe refers to Sections 1798.81.5 and 1798.82 as the “California Data Breach Notification Act,”
 26 see Mot. at 6, whereas Plaintiffs refer to those sections as the “California Customer Records Act,”
 27 see Opp’n at 6. The Court agrees with Plaintiffs that Section 1798.81.5 deals with more than
 28 notification in the event of a breach. See Cal. Civ. Code § 1798.81.5(d) (“[T]he purpose of this
 section is to encourage businesses that own or license personal information about Californians to
 provide reasonable security for that information.”). Accordingly, the Court will refer to these
 sections as the Customer Records Act (“CRA”), after the name of the Title under which they
 appear. See Cal. Civ. Code tit. 1.81 (“Customer Records”).

1 customers following the 2013 data breach, in violation of Section 1798.82 of the CRA. Compl.
2 ¶¶ 112-113.

3 Plaintiffs request injunctive relief pursuant to Section 1798.84(e) of the CRA, which
4 provides that “[a]ny business that violates, proposes to violate, or has violated this title may be
5 enjoined.” Plaintiffs also base their request for relief on the “unlawful” prong of California’s
6 Unfair Competition Law (“UCL”), Cal. Bus. & Prof. Code §§ 17200 *et seq.*, which allows
7 plaintiffs to “borrow” violations of other laws and treat them as unlawful competition that is
8 independently actionable. *Cel-Tech Commcn’s, Inc. v. L.A. Cellular Tel. Co.*, 20 Cal. 4th 163, 180
9 (1999).

10 Adobe argues that Plaintiffs do not allege injury-in-fact resulting from Adobe’s alleged
11 violation of the CRA and thus do not have Article III standing to bring their CRA claim. Mot. at 6-
12 7. For the same reasons, Adobe contends that Plaintiffs do not have statutory standing under
13 Section 1798.84(e), which also requires a showing of injury. *Id.* As a result, Adobe contends that
14 Plaintiffs’ CRA claim must be dismissed for lack of jurisdiction. The Court addresses both
15 contentions in turn, beginning, as it must, with Article III standing.

16 **1. Article III Standing**

17 To have Article III standing, a plaintiff must plead and prove that she has suffered sufficient
18 injury to satisfy the “case or controversy” requirement of Article III of the United States
19 Constitution. *See Clapper v. Amnesty Int’l USA*, --- U.S. ---, 133 S. Ct. 1138, 1146 (2013) (“One
20 element of the case-or-controversy requirement’ is that plaintiffs ‘must establish that they have
21 standing to sue.’” (quoting *Raines v. Byrd*, 521 U.S. 811, 818 (1997))). To satisfy Article III
22 standing, a plaintiff must therefore allege: (1) injury-in-fact that is concrete and particularized, as
23 well as actual or imminent; (2) that the injury is fairly traceable to the challenged action of the
24 defendant; and (3) that the injury is redressable by a favorable ruling. *Monsanto Co. v. Geertson*
25 *Seed Farms*, 561 U.S. 139, 149 (2010); *Friends of the Earth, Inc. v. Laidlaw Env’tl. Servs. (TOC),*
26 *Inc.*, 528 U.S. 167, 180-81 (2000). “The party invoking federal jurisdiction bears the burden of
27
28

1 establishing these elements . . . with the manner and degree of evidence required at the successive
2 stages of the litigation.” *Lujan*, 504 U.S. at 561.

3 In a class action, named plaintiffs representing a class “must allege and show that they
4 personally have been injured, not that injury has been suffered by other, unidentified members of
5 the class to which they belong and which they purport to represent.” *Warth v. Seldin*, 422 U.S. 490,
6 502 (1975). “[I]f none of the named plaintiffs purporting to represent a class establishes the
7 requisite of a case or controversy with the defendants, none may seek relief on behalf of himself or
8 any other member of the class.” *O’Shea v. Littleton*, 414 U.S. 488, 494 (1974).

9 In the instant case, Plaintiffs allege that they have all suffered at least one of three types of
10 cognizable injuries-in-fact: (1) increased risk of future harm; (2) cost to mitigate the risk of future
11 harm; and/or (3) loss of the value of their Adobe products. Opp’n at 7-11. The Court begins by
12 assessing the adequacy Plaintiffs’ alleged injuries. The Court will then address Adobe’s argument
13 that even if Plaintiffs have Article III standing to bring a claim based on Adobe’s alleged violation
14 of Section 1798.81.5 (the “reasonable” security measures provision), Plaintiffs do not have
15 standing to bring a claim based on Adobe’s alleged violation of Section 1798.82 (the notification
16 provision), because Plaintiffs do not allege that they suffered any particular injury stemming from
17 Adobe’s failure to reasonably *notify* Plaintiffs of the 2013 data breach. Mot. at 7.

18 **a. Increased Risk of Harm**

19 Plaintiffs claim that they are all at increased risk of future harm as a result of the 2013 data
20 breach. Opp’n at 7. Adobe counters that such “increased risk” is not a cognizable injury for Article
21 III standing purposes. Mot. at 10. The Ninth Circuit addressed Article III standing in the context of
22 stolen personal information in *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010). In
23 *Krottner*, a thief stole a laptop from Starbucks containing the unencrypted names, addresses, and
24 social security numbers of roughly 97,000 Starbucks employees. *Id.* at 1140. Some of the affected
25 employees subsequently sued Starbucks for negligence and breach of implied contract. *Id.*
26 Starbucks argued that the employees did not have standing because there was no indication that
27 any of the employees’ personal information had been misused or that the employees had suffered
28

1 any economic loss as a result of the theft. *Id.* at 1141-42. The Ninth Circuit disagreed, holding
2 instead that “the possibility of future injury may be sufficient to confer standing” where the
3 plaintiff is “*immediately* in danger of sustaining some *direct* injury as the result of the challenged
4 conduct.” *Id.* at 1142 (alteration omitted) (internal quotation marks omitted). As to the specific
5 facts before it, the Ninth Circuit held that the Starbucks employees alleged “a credible threat of real
6 and immediate harm stemming from the theft of a laptop containing their unencrypted personal
7 data.” *Id.* at 1143. Based on this “credible threat of real and immediate harm,” the Ninth Circuit
8 found that the employees “sufficiently alleged an injury-in-fact for purposes of Article III
9 standing.” *Id.*

10 Adobe does not dispute that *Krottner* is directly on point. *See* Mot. at 11; Reply at 3.
11 However, Adobe contends that subsequent Supreme Court authority forecloses the approach the
12 Ninth Circuit took to standing in *Krottner*. Reply at 3. Specifically, Adobe claims that the Supreme
13 Court’s decision in *Clapper v. Amnesty International USA* expressly rejected “[a]llegations of
14 possible future injury” as a basis for Article III standing, requiring instead that a “threatened injury
15 [] be *certainly impending* to constitute injury in fact.” Mot. at 10 (citing *Clapper*, 133 S. Ct. at
16 1147). Adobe argues that following *Clapper* district courts in data breach cases regularly conclude
17 that increased risk of future harm is insufficient to confer Article III standing under the “certainly
18 impending” standard. *Id.* (citing *In re Sci. Applications Int’l Corp. Backup Tape Data Theft Litig.*
19 (“SAIC”), --- F. Supp. 2d ---, 2014 WL 1858458 (D.D.C. May 9, 2014); *Strautins v. Trustwave*
20 *Holdings, Inc.*, --- F. Supp. 2d ---, 2014 WL 960816 (N.D. Ill. Mar. 12, 2014); *Galaria v.*
21 *Nationwide Mut. Ins. Co.*, --- F. Supp. 2d ---, 2014 WL 689703 (S.D. Ohio Feb. 10, 2014); *Polanco*
22 *v. Omnicell, Inc.*, 988 F. Supp. 2d 451 (D.N.J. 2013); *In re Barnes & Noble Pin Pad Litig.*, No. 12-
23 8617, 2013 WL 4759588 (N.D. Ill. Sep. 3, 2013); *Yunker v. Pandora Media, Inc.*, No. 11-3113,
24 2013 WL 1282980 (N.D. Cal. Mar. 26, 2013)). Adobe claims that the only case to hold otherwise,
25 *In re Sony Gaming Networks & Customer Data Security Breach Litigation*, --- F. Supp. 2d ---,
26 2014 WL 223677 (S.D. Cal. Jan 21, 2014), has been “relegated to a ‘*but see*’ reference.” Mot. at 11
27 (citing SAIC, 2014 WL 1858458, at *8). Adobe encourages this Court to conclude that *Clapper*
28

1 implicitly overruled *Krottner* and to join the district courts that have rejected the “increased risk of
2 harm” theory of standing in *Clapper*’s wake. *Id.* at 10-11. For the following reasons, the Court
3 declines to do so.

4 *Clapper* addressed a challenge to Section 702 of the Foreign Intelligence Surveillance Act
5 of 1978 (“FISA”), 50 U.S.C. § 1881a. 133 S. Ct. at 1142. Respondents were U.S.-based attorneys,
6 human rights, labor, legal, and media organizations who alleged that their work required them to
7 communicate with individuals outside the United States who were likely to be targets of
8 surveillance under Section 702. *Id.* at 1145. The respondents asserted injury based on “an
9 objectively reasonable likelihood that their communications [would] be acquired [under FISA] at
10 some point in the future.” *Id.* at 1146. As an initial matter, the Supreme Court held that the
11 “objectively reasonable likelihood” standard was inconsistent with precedent requiring that
12 “threatened injury must be *certainly impending* to constitute injury in fact.” *Id.* at 1147 (emphasis
13 added) (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990)). The Supreme Court emphasized
14 that “allegations of *possible* future injury are not sufficient.” *Id.* (internal quotation marks omitted).
15 Turning to the respondents’ theory of injury, the Supreme Court found that it was both too
16 speculative to constitute “certainly impending” injury and too attenuated to be “fairly traceable” to
17 Section 702. *Id.* at 1147-48.

18 As the Supreme Court noted, the respondents did not allege that any of their
19 communications had actually been intercepted, or even that the Government sought to target them
20 directly. *Id.* at 1148. Rather, the respondents’ argument rested on the “highly speculative fear” that:

21 (1) the Government will decide to target the communications of non-U.S. persons
22 with whom they communicate; (2) in doing so, the Government will choose to
23 invoke its authority under [Section 702] rather than utilizing another method of
24 surveillance; (3) the Article III judges who serve on the Foreign Intelligence
25 Surveillance Court will conclude that the Government’s proposed surveillance
26 procedures satisfy [Section 702]’s many safeguards and are consistent with the
27 Fourth Amendment; (4) the Government will succeed in intercepting the
28 communications of respondents’ contacts; and (5) respondents will be parties to the
particular communications that the Government intercepts

Id. The Supreme Court held that this “highly attenuated” chain of possibilities did not result in a
“certainly impending” injury. *Id.* The Court observed that the first three steps of the chain

1 depended on the independent choices of the Government and the Foreign Intelligence Surveillance
 2 Court, yet the respondents could only speculate as to what decision those third parties would take
 3 at each step. *Id.* at 1149-50 (“[W]e have been reluctant to endorse standing theories that require
 4 guesswork as to how independent decisionmakers will exercise their judgment. . . .”). Moreover,
 5 respondents could not show with any certainty that *their* communications with the foreign persons
 6 allegedly under surveillance would be intercepted. *Id.* As a result, the overall chain of inferences
 7 was “too speculative” to constitute a cognizable injury. *Id.* at 1143.

8 The Supreme Court acknowledged that its precedents “do not uniformly require plaintiffs to
 9 demonstrate that it is *literally certain* that the harms they identify will come about” in order to have
 10 standing. *Id.* at 1150 n.5 (emphasis added). Rather, in some cases, the Supreme Court has found
 11 standing “based on a ‘substantial risk’ that the harm will occur, which may prompt plaintiffs to
 12 reasonably incur costs to mitigate or avoid that harm.” *Id.* (citing *Monsanto*, 561 U.S. at 153-54;
 13 *Pennell v. City of San Jose*, 485 U.S. 1, 8 (1988); *Blum v. Yaretsky*, 457 U.S. 991, 1000-01 (1982);
 14 *Babbitt v. Farm Workers*, 442 U.S. 289, 298 (1979)). The Supreme Court declined to overrule that
 15 line of cases. However, the Court concluded in *Clapper* that “to the extent that the ‘substantial risk’
 16 standard is relevant and is distinct from the ‘clearly impending’ requirement, respondents fall short
 17 of even that standard, in light of the attenuated chain of inferences necessary to find harm here.” *Id.*

18 *Clapper* did not change the law governing Article III standing. The Supreme Court did not
 19 overrule any precedent, nor did it reformulate the familiar standing requirements of injury-in-fact,
 20 causation, and redressability.⁴ *Accord Sony*, 2014 WL 223677, at *8-9 (“[T]he Supreme Court’s
 21 decision in *Clapper* did not set forth a new Article III framework, nor did the Supreme Court’s
 22 decision overrule previous precedent”). *Clapper* merely held that the Second Circuit had
 23 strayed from these well-established standing principles by accepting a too-speculative theory of
 24 future injury. *See* 133 S. Ct. at 1146 (characterizing the Second Circuit’s view of standing as
 25 “novel”). In the absence of any indication in *Clapper* that the Supreme Court intended a wide-

26
 27 ⁴ Indeed, the “certainly impending” language can be traced back to a 1923 decision, *Pennsylvania*
 28 *v. West Virginia*, 262 U.S. 553, 593 (1923), and has been cited numerous times in U.S. Supreme
 Court cases addressing standing in the intervening decades. *See, e.g., Lujan*, 504 U.S. at 564 n.2;
Whitmore, 495 U.S. at 158; *Babbitt*, 442 U.S. at 298.

1 reaching revision to existing standing doctrine, the Court is reluctant to conclude that *Clapper*
2 represents the sea change that Adobe suggests. Moreover, *Clapper*'s discussion of standing arose
3 in the sensitive context of a claim that other branches of government were violating the
4 Constitution, and the U.S. Supreme Court itself noted that its standing analysis was unusually
5 rigorous as a result. *Id.* at 1147 (“Our standing inquiry has been especially rigorous when reaching
6 the merits of the dispute would force us to decide whether an action taken by one of the other two
7 branches of the Federal Government was unconstitutional.” (alteration omitted) (internal quotation
8 marks omitted)).

9 “[D]istrict courts should consider themselves bound by [] intervening higher authority and
10 reject the prior opinion of [the Ninth Circuit] as having been effectively overruled” only when the
11 intervening higher authority is “clearly irreconcilable with [the] prior circuit authority.” *Miller v.*
12 *Gammie*, 335 F.3d 889, 900 (9th Cir. 2003) (en banc). The Court does not find that *Krottner* and
13 *Clapper* are clearly irreconcilable. *Krottner* did use somewhat different phrases to describe the
14 degree of imminence a plaintiff must allege in order to have standing based on a threat of injury,
15 *i.e.*, “immediate[] [] danger of sustaining some direct injury,” and a “credible threat of real and
16 immediate harm.” 628 F.3d at 1142-43. On the other hand, *Clapper* described the harm as
17 “certainly impending.” 133 S. Ct. at 1147. However, this difference in wording is not substantial.
18 At the least, the Court finds that *Krottner*'s phrasing is closer to *Clapper*'s “certainly impending”
19 language than it is to the Second Circuit's “objective reasonable likelihood” standard that the
20 Supreme Court reversed in *Clapper*. Given that *Krottner* described the imminence standard in
21 terms similar to those used in *Clapper*, and in light of the fact that nothing in *Clapper* reveals an
22 intent to alter established standing principles, the Court cannot conclude that *Krottner* has been
23 effectively overruled.

24 In any event, even if *Krottner* is no longer good law, the threatened harm alleged here is
25 sufficiently concrete and imminent to satisfy *Clapper*. Unlike in *Clapper*, where respondents'
26 claim that they would suffer future harm rested on a chain of events that was both “highly
27 attenuated” and “highly speculative,” 133 S. Ct. at 1148, the risk that Plaintiffs' personal data will
28

1 be misused by the hackers who breached Adobe's network is immediate and very real. Plaintiffs
2 allege that the hackers deliberately targeted Adobe's servers and spent several weeks collecting
3 names, usernames, passwords, email addresses, phone numbers, mailing addresses, and credit card
4 numbers and expiration dates. Compl. ¶¶ 48, 50. Plaintiffs' personal information was among the
5 information taken during the breach. *Id.* ¶¶ 76, 80, 85, 92, 97, 100. Thus, in contrast to *Clapper*,
6 where there was no evidence that any of respondents' communications either had been or would be
7 monitored under Section 702, *see* 133 S. Ct. at 1148, here there is no need to speculate as to
8 whether Plaintiffs' information has been stolen and what information was taken.

9 Neither is there any need to speculate as to whether the hackers intend to misuse the
10 personal information stolen in the 2013 data breach or whether they will be able to do so. Not only
11 did the hackers deliberately target Adobe's servers, but Plaintiffs allege that the hackers used
12 Adobe's own systems to decrypt customer credit card numbers. Compl. ¶ 57. Some of the stolen
13 data has already surfaced on the Internet, and other hackers have allegedly misused it to discover
14 vulnerabilities in Adobe's products. *Id.* ¶¶ 49, 70. Given this, the danger that Plaintiffs' stolen data
15 will be subject to misuse can plausibly be described as "certainly impending." Indeed, the
16 threatened injury here could be more imminent only if Plaintiffs could allege that their stolen
17 personal information had already been misused. However, to require Plaintiffs to wait until they
18 actually suffer identity theft or credit card fraud in order to have standing would run counter to the
19 well-established principle that harm need not have already occurred or be "literally certain" in
20 order to constitute injury-in-fact.⁵ *Clapper*, 133 S. Ct. at 1150 n.5; *see also, e.g., Monsanto*, 561

21
22
23
24
25
26
27
28

⁵ The Court further notes that requiring Plaintiffs to wait for the threatened harm to materialize in order to sue would pose a standing problem of its own, because the more time that passes between a data breach and an instance of identity theft, the more latitude a defendant has to argue that the identity theft is not "fairly traceable" to the defendant's data breach. Indeed, Adobe makes this very argument in its Motion. Specifically, Adobe speculates that Plaintiff Halpain may also have been a victim of recent data breaches involving Target and Neiman Marcus, and thus that Halpain's allegation that her personal data appeared on "black market websites" is not fairly traceable to Adobe's 2013 data breach. Mot. at 9 & n.8. This argument fails, given that there is no factual basis for Adobe's speculation that Halpain was a customer of either Target or Neiman Marcus, let alone that Halpain's personal data was compromised in data breaches involving these companies.

1 U.S. at 153-54 (finding that a “substantial risk of gene flow” from genetically engineered alfalfa
2 crops to non-genetically engineered alfalfa crops was sufficient to confer Article III standing).⁶

3 The cases Adobe cites in which district courts have relied on *Clapper* to dismiss data
4 breach cases on standing grounds are factually distinct from the present case. In *SAIC*, the case on
5 which Adobe most heavily relies, a thief broke into a car in San Antonio, Texas and stole the car’s
6 GPS and stereo, as well as encrypted backup data tapes containing personal medical information
7 for over four million U.S. military members and their families. 2014 WL 1858458, at *2. As the
8 *SAIC* court found, the thief would need to have recognized the data tapes for what they were,
9 obtained specialized equipment to read the tapes, broken the encryption protecting the data on the
10 tapes, and then obtained specialized software to read the data, all before being in any position to
11 misuse the data. *Id.* at *6. Such a chain of possibilities, the *SAIC* court held, was as attenuated as
12 the chain the Supreme Court rejected in *Clapper*, especially given the more likely possibility that
13 the thief had simply sold the GPS and stereo and discarded the data tapes “in a landfill somewhere
14 in Texas.” *Id.* The facts of *SAIC* stand in sharp contrast to those alleged here, where hackers
15 targeted Adobe’s servers in order to steal customer data, at least some of that data has been
16 successfully decrypted, and some of the information stolen in the 2013 data breach has already
17 surfaced on websites used by hackers.

18 Adobe’s other authorities are similarly distinct. The thief in *Polanco* also stole a laptop out
19 of a car. 988 F. Supp. 2d at 456. Again, there was no allegation that the thief targeted the laptop for
20 the data contained therein, and the plaintiff “essentially concede[d]” that she had not alleged “any
21 misuse of her [personal information] or [] that she [wa]s now at an increased risk for the misuse of
22 her information in the future based on the theft of the laptop.” *Id.* at 467. In both *Strautins* and
23 *Barnes & Noble*, it was unclear if the plaintiffs’ information had been taken at all. 2014 WL
24 960816, at *6-7; 2013 WL 4759588, at *4. Finally, in *Yunker*, the plaintiff did not allege that he
25

26
27 ⁶ It is also worth noting that *Clapper* was decided on summary judgment, *see* 133 S. Ct. at 1146,
28 which requires that a plaintiff come forward with a greater degree of evidentiary proof to support
her standing allegations than is required at the motion to dismiss stage, *see Lujan*, 504 U.S. at 561.

1 had provided any sensitive information (such as a credit card number or a social security number)
2 or that anyone had breached the defendant's servers. 2013 WL 1282980, at *5.

3 The case with facts closest to those at issue here is *Galaria*. In that case, hackers obtained a
4 variety of personal information, though not credit card information, from the servers of an
5 insurance company. *Galaria*, 2014 WL 689703, at *1. The court declined to find standing based on
6 increased risk of future harm, reasoning that whether plaintiffs would be harmed depended on the
7 decision of the unknown hackers, who may or may not attempt to misuse the stolen information.
8 *Id.* at *6. The Court finds this reasoning unpersuasive—after all, why would hackers target and
9 steal personal customer data if not to misuse it?—and declines to follow it. Regardless, *Galaria*'s
10 reasoning lacks force here, where Plaintiffs allege that some of the stolen data has already been
11 misused. *See* Compl. ¶¶ 49, 70.

12 In sum, the Court finds that Plaintiffs' allegations of a concrete and imminent threat of
13 future harm suffice to establish Article III injury-in-fact at the pleadings stage under both *Krottner*
14 and *Clapper*.

15 **b. Cost to Mitigate**

16 In addition, Plaintiffs allege that Plaintiffs Halpain and Kar have standing based on the
17 reasonable costs they incurred to mitigate the increased risk of harm resulting from the 2013 data
18 breach. Opp'n at 10; *see* Compl. ¶¶ 80-81, 86-87 (alleging that Halpain and Kar paid for data
19 monitoring services). The Supreme Court held in *Clapper* that plaintiffs "cannot manufacture
20 standing merely by inflicting harm on themselves based on their fears of hypothetical future harm
21 that is not certainly impending." 133 S. Ct. at 1151. In so holding, the Supreme Court rejected the
22 *Clapper* respondents' argument that they had standing because they had taken on costly and
23 burdensome measures to protect the confidentiality of their communications. *Id.* Even where the
24 fear of harm was not "fanciful, paranoid, or otherwise unreasonable," the Supreme Court noted,
25 plaintiffs cannot secure a lower standard for standing "simply by making an expenditure based on
26 [that] fear." *Id.*

1 As this last quote indicates, the Supreme Court’s primary concern was that the Article III
 2 standing standard would be “water[ed] down” if a plaintiff who otherwise lacked standing could
 3 manufacture an injury-in-fact “for the price of a plane ticket.” *Id.* (internal quotation marks
 4 omitted); *accord SAIC*, 2014 WL 1858458, at *7 (“Put another way, the [Supreme] Court has held
 5 that plaintiffs cannot create standing by ‘inflicting harm on themselves’ to ward off an otherwise
 6 speculative injury.” (quoting *Clapper*, 133 S. Ct. at 1151)). Therefore, in order for costs incurred in
 7 an effort to mitigate the risk of future harm to constitute injury-in-fact, the future harm being
 8 mitigated must itself be imminent.⁷ As the Court has found that all Plaintiffs adequately alleged
 9 that they face a certainly impending future harm from the theft of their personal data, *see supra*
 10 Part III.A.1.a, the Court finds that the costs Plaintiffs Halpain and Kar incurred to mitigate this
 11 future harm constitute an additional injury-in-fact.⁸

12 For the foregoing reasons, the Court finds that Plaintiffs have plausibly alleged that the
 13 substantial risk of harm Plaintiffs face following the 2013 data breach constitutes a cognizable
 14 injury-in-fact. The costs Plaintiffs Halpain and Kar incurred to mitigate this risk of harm constitute
 15 an additional cognizable injury. The Court further finds that Plaintiffs plausibly allege both that
 16 these injuries are “fairly traceable” to Adobe’s alleged failure to maintain “reasonable” security
 17 measures in violation of Section 1798.81.5 and that the relief sought would redress these injuries.

18 ⁷ The precise degree of imminence required is somewhat uncertain. While a “certainly impending”
 19 risk of future harm would undoubtedly be sufficiently imminent to confer standing on a plaintiff
 20 who took costly measures to mitigate that risk, *Clapper* did not overrule prior cases that have found
 21 standing where a plaintiff incurs costs in order to mitigate a risk of harm that is “substantial.” 133
 22 S. Ct. at 1150 n.5 (there can be standing “based on a ‘substantial risk’ that the harm will occur,
 23 which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm”). The
 24 *Clapper* Court declined, however, to determine whether a “substantial” risk of future harm is
 25 meaningfully different from a “certainly impending” risk of future harm. *See id.* (“But to the extent
 26 that the ‘substantial risk’ standard is relevant and is distinct from the ‘clearly impending’
 27 requirement, respondents fall short of even that standard, in light of the attenuated chain of
 28 inferences necessary to find harm here.”). This Court need not resolve whether there is any
 practical difference between the two formulations either, as the Court finds that Plaintiffs’
 allegations meet the “certainly impending” standard.

⁸ Plaintiffs additionally allege that they suffered economic injury in the form of lost value, both
 because the software Plaintiffs paid for is now “highly vulnerable to attacks,” and because
 Plaintiffs Halpain and McGlynn would not have subscribed to Creative Cloud had they known of
 Adobe’s substandard security practices. *See Opp’n* at 10. As the Court has already found that all
 Plaintiffs have Article III standing to pursue their CRA claims based on an increased risk of harm
 and, in the case of Plaintiffs Halpain and Kar, costs incurred to mitigate that risk of harm, the Court
 need not address this additional theory of standing.

1 The Court therefore concludes that Plaintiffs have adequately pleaded that they have Article III
2 standing to bring a CRA claim for violations of Section 1798.81.5.

3 **c. Section 1798.82**

4 Adobe argues that even if Plaintiffs have adequately alleged injury-in-fact stemming from
5 Adobe's alleged failure to implement reasonable security measures, Plaintiffs have not alleged any
6 injury traceable to Adobe's alleged failure to reasonably *notify* customers of the 2013 data breach
7 in violation of Section 1798.82, because Plaintiffs do not allege that they suffered any incremental
8 harm as a result of the delay. Mot. at 7. The Court agrees that Plaintiffs do not allege any harm
9 resulting from the delay in their Complaint, and Plaintiffs do not address this argument in their
10 Opposition except to argue that they have statutory (as opposed to Article III) standing to bring a
11 Section 1798.82 claim. *See* Opp'n at 11.

12 Article III's standing requirements are mandatory and separate from any statutory standing
13 requirements. Article III standing is also claim- and relief-specific, such that a plaintiff must
14 establish Article III standing for each of her claims and for each form of relief sought. *See*
15 *DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 352 (2006) (“[O]ur standing cases confirm that a
16 plaintiff must demonstrate standing for each claim he seeks to press.”); *id.* (“We have insisted . . .
17 that a plaintiff must demonstrate standing separately for each form of relief sought.” (internal
18 quotation marks omitted)). Plaintiffs’ claim that Adobe failed to reasonably notify its customers of
19 the 2013 data breach is distinct from Plaintiffs’ claim that Adobe failed to maintain reasonable data
20 security measures—in that the claims arise under different statutory provisions and challenge
21 different Adobe conduct—and Plaintiffs seek different injunctive relief to remedy each violation.
22 *Compare* Compl. ¶ 116 (seeking injunction ordering Adobe to implement various security
23 measures), *with id.* ¶ 117 (seeking injunction ordering Adobe to notify customers affected by the
24 2013 data breach who have not yet received notice that their data was stolen). Thus, the Court
25 concludes that Plaintiffs must separately establish Article III standing under Section 1798.82.
26 However, by failing to allege any injury resulting from a failure to provide reasonable notification
27 of the 2013 data breach, Plaintiffs have not plausibly alleged that they have standing to pursue a
28

1 Section 1798.82 claim. Accordingly, the Court GRANTS Adobe's Motion to Dismiss Plaintiffs'
2 Section 1798.82 claim for lacking of Article III standing. Because Plaintiffs may be able to cure
3 this deficiency in an amended complaint, this dismissal is without prejudice.

4 **2. Statutory Standing**

5 The CRA also contains a statutory standing requirement. Section 1798.84, the remedies
6 provision of the CRA, provides that "[a]ny customer injured by a violation of this title may
7 institute a civil action to recover damages," Cal. Civ. Code § 1798.84(b), and the California Court
8 of Appeal has held that this injury requirement applies "regardless of the remedies [a plaintiff]
9 seek[s]," *Boorstein v. CBS Interactive, Inc.*, 222 Cal. App. 4th 456, 466-67 (2013); *accord Murray*
10 *v. Time Inc.*, 554 F. App'x 654, 655 (9th Cir. 2014). Therefore, where a plaintiff fails to allege a
11 cognizable injury, the plaintiff "lacks statutory standing" to bring a claim under Section 1798.84,
12 "regardless of whether [the] allegations are sufficient to state a violation of the [statute]." *Boorstein*,
13 222 Cal. App. 4th at 467 (internal quotation marks omitted).

14 Although Section 1798.84 does not define what qualifies as an injury under the statute,
15 other courts in the Ninth Circuit have found that an injury that satisfies Article III's injury-in-fact
16 standard suffices to establish statutory injury under the CRA. *See, e.g., Miller v. Hearst Commc'ns,*
17 *Inc.*, No. 12-733, 2012 WL 3205241, at *6 (C.D. Cal. Aug. 3, 2012); *Boorstein v. Men's Journal*
18 *LLC*, No 12-771, 2012 WL 2152815, at *3-4 (C.D. Cal. June 14, 2012). As Adobe does not
19 contend, and as the Court has no reason to believe, that the CRA's statutory standing requirements
20 are more stringent than Article III's, the Court finds that Plaintiffs' allegations of injury-in-fact
21 satisfy the CRA's statutory standing requirement for the same reasons these allegations satisfy
22 Article III. *See supra* Part III.A.1.

23 In summary, the Court DENIES Adobe's Motion to Dismiss Plaintiffs' CRA claim for
24 violations of Section 1798.81.5. The Court GRANTS Adobe's Motion to Dismiss Plaintiffs' CRA
25 claim for violations of Section 1798.82 without prejudice.

1 **B. Declaratory Relief**

2 Plaintiffs’ second cause of action is for declaratory relief on behalf of all Plaintiffs. Compl.
3 ¶¶ 118-124. As a preliminary matter, the parties disagree over whether the federal Declaratory
4 Judgment Act, 28 U.S.C. § 2201, applies, as Adobe contends, or if the California Declaratory
5 Relief Act, Cal. Civ. Proc. Code § 1060, applies, as Plaintiffs contend. *Compare* Reply at 5 n.4,
6 *with* Opp’n at 14.

7 The Court finds that the federal Declaratory Judgment Act governs in this case. Although
8 district courts in the Ninth Circuit have at times applied the California Declaratory Relief Act when
9 sitting in diversity, *see Valley Forge Ins. Co. v. APL Co. Pte. Ltd.*, No. 09-9323, 2010 WL 960341,
10 at *4 n.5 (C.D. Cal. Mar. 16, 2010) (citing cases), other district courts apply the federal Act, *see*,
11 *e.g., DeFeo v. Procter & Gamble Co.*, 831 F. Supp. 776, 779 (N.D. Cal. 1993) (“The propriety of
12 granting declaratory relief in federal court is a procedural matter. . . . Therefore, the Declaratory
13 Judgment Act is implicated even in diversity cases” (citations omitted)). For its part, the Ninth
14 Circuit has indicated, although not explicitly held, that the federal Declaratory Judgment Act
15 should apply. In *Golden Eagle Insurance Co. v. Travelers Cos.*, 103 F.3d 750, 753 (9th Cir. 1996),
16 *overruled on other grounds by Gov’t Emps. Ins. Co. v. Dizol*, 133 F.3d 1220 (1998) (en banc), the
17 Ninth Circuit stated that although “[t]he complaint [plaintiff] filed in state court was for declaratory
18 relief under California’s declaratory relief statute,” “[w]hen [defendant] removed the case to
19 federal court, based on diversity of citizenship, the claim remained one for declaratory relief, but
20 the question whether to exercise federal jurisdiction to resolve the controversy became a procedural
21 question of federal law.” Finally, the U.S. Supreme Court has emphasized the procedural nature of
22 the Declaratory Judgment Act, which further supports the conclusion that the federal Act applies.
23 *See Skelly Oil Co. v. Phillips Petroleum Co.*, 339 U.S. 667, 671 (1950) (“[T]he operation of the
24 Declaratory Judgment Act is procedural only.” (quoting *Aetna Life Ins. Co. v. Haworth*, 200 U.S.
25 227, 240 (1937))). The Court will therefore consider Plaintiffs’ declaratory relief claim under the
26 federal Declaratory Judgment Act. In any event, as Plaintiffs acknowledge, whether the state or
27
28

1 federal statute applies makes little difference as a practical matter, as the two statutes are broadly
2 equivalent.⁹ *See* Opp'n at 14.

3 The federal Declaratory Judgment Act provides that “[i]n a case of actual controversy
4 within its jurisdiction . . . any court of the United States . . . may declare the rights and other legal
5 relations of any interested party seeking such declaration, whether or not further relief is or could
6 be sought.” 28 U.S.C. § 2201(a). To fall within the Act’s ambit, the “case of actual controversy”
7 must be “‘definite and concrete, touching the legal relations of parties having adverse legal
8 interests,’ . . . ‘real and substantial’ and ‘admi[t] of specific relief through a decree of a conclusive
9 character, as distinguished from an opinion advising what the law would be upon a hypothetical
10 state of facts.’” *MedImmune, Inc. v. Genentech, Inc.*, 549 U.S. 118, 127 (2007) (alteration in
11 original) (quoting *Aetna Life*, 300 U.S. at 240-241). Plaintiffs seek a declaration that: (a) Adobe
12 fails to fulfill its existing contractual obligation to provide reasonable security measures; and (b) to
13 comply with its contractual obligations, Adobe must implement specified additional security
14 measures. Compl. ¶ 124.

15 Adobe moves to dismiss Plaintiff’s declaratory relief claim on three grounds. First, Adobe
16 asserts that Plaintiffs have not suffered an injury-in-fact and therefore lack standing. Mot. at 13.
17 Second, Adobe contends that what Plaintiffs actually seek is an impermissible advisory opinion
18 that lays the foundation for future litigation, rather than adjudication of an actual controversy
19 between the parties. *Id.* at 13-14. Third, Adobe argues that Plaintiffs’ declaratory relief claim is
20 actually a breach of contract claim in disguise, and that the claim fails because Plaintiffs have
21 failed to plead all the elements of a breach of contract claim. *Id.* at 15. The Court addresses each
22 contention in turn.

23
24
25
26
27
28

⁹ Compare 28 U.S.C. § 2201 (“In a case of actual controversy within its jurisdiction . . . any court of the United States, upon the filing of an appropriate pleading, may declare the rights and other legal relations of any interested party seeking such declaration, whether or not further relief is or could be sought.”), with Cal. Civ. Proc. Code § 1060 (“Any person interested under a written instrument . . . or under a contract . . . may, in cases of actual controversy relating to the legal rights and duties of the respective parties, bring an original action . . . for a declaration of his or her rights and duties [T]he court may make a binding declaration of these rights or duties, whether or not further relief is or could be claimed at the time.”).

1. Article III Standing

1 Adobe first claims that, just as the California Plaintiffs fail to allege injury-in-fact for
2 purposes of their CRA claim, the California Plaintiffs fail to allege a cognizable injury-in-fact for
3 purposes of declaratory relief. Mot. at 13; *see also Dizol*, 133 F.3d at 1222-23 (“A lawsuit seeking
4 federal declaratory relief must first present an actual case or controversy within the meaning of
5 Article III, section 2 of the United States Constitution. . . . It must also fulfill statutory
6 jurisdictional prerequisites.” (citation omitted)). In addition, Adobe claims that the non-California
7 Plaintiffs do not allege any injury whatsoever. Mot. at 13. Adobe argues that therefore none of the
8 Plaintiffs alleges injury-in-fact that is fairly traceable to Adobe’s failure to abide by its contractual
9 obligations. *Id.*

10
11 The Court finds that Plaintiffs have adequately pleaded that they have Article III standing to
12 bring a claim for declaratory relief. First, as discussed above, the Court finds that all Plaintiffs have
13 plausibly alleged that they face a substantial, “certainly impending” risk of harm from the 2013
14 data breach. *See supra* Part III.A.1.a. This alleged injury is fairly traceable to Adobe’s failure to
15 abide by its contractual obligation to provide “reasonable . . . security controls,” Agreement at 4,
16 and will plausibly be redressed by the declaratory relief Plaintiffs seek. Accordingly, the Court
17 declines to dismiss Plaintiffs’ declaratory relief claim for lack of Article III standing.

2. Presence of an Actionable Dispute

18
19 Adobe next seeks dismissal of Plaintiffs’ declaratory relief claim on the ground that
20 Plaintiffs do not fulfill the Declaratory Judgment Act’s statutory jurisdictional requirements. Adobe
21 contends that there is no actionable dispute over whether Adobe is in breach of its contractual
22 obligation to provide “reasonable . . . security controls,” given that the Agreement expressly
23 provides that no security measure is “100%” effective and that “Adobe cannot ensure or warrant
24 the security of your personal information.” Mot. at 14. Adobe further contends that Plaintiffs do not
25 allege that a declaration of rights is necessary at this time. *Id.* Adobe asserts that Plaintiffs’ claim is
26 consequently unripe, and is instead a request for an impermissible advisory opinion. *Id.* Adobe
27
28

1 contends that what Plaintiffs actually seek is an advantage for future litigation by obtaining an
2 “advance ruling.” *Id.*

3 A claim for relief under the Declaratory Judgment Act requires a dispute that is: (1)
4 “definite and concrete, touching the legal relations of parties having adverse legal interests”; (2)
5 “real and substantial”; and (3) “admit[ting] of specific relief through a decree of a conclusive
6 character, as distinguished from an opinion advising what the law would be upon a hypothetical
7 state of facts.” *MedImmune*, 549 U.S. at 127 (internal quotation marks omitted). The Supreme
8 Court has admitted that “not . . . the brightest of lines” separates cases that satisfy the statutory
9 jurisdictional requirements and those that do not. *Id.* The central question, however, is whether
10 “the facts alleged, under all the circumstances, show that there is a substantial controversy,
11 between parties having adverse legal interests, of sufficient immediacy and reality to warrant the
12 issuance of a declaratory judgment.” *Id.* (quoting *Md. Cas. Co. v. Pac. Coal & Oil Co.*, 312 U.S.
13 270, 273 (1941)).

14 The Court finds that Plaintiffs have adequately alleged the existence of an actionable
15 dispute for purposes of the Declaratory Judgment Act. Plaintiffs have plausibly alleged the
16 existence of a “definite and concrete” dispute over the meaning and the scope of Adobe’s
17 contractual obligation to provide “reasonable” security measures. *See* Compl. ¶¶ 120-123.
18 According to the Complaint, although “Adobe maintains that its security measures were adequate
19 and remain adequate,” there were in fact a number of standard industry practices that Adobe failed
20 to follow. *Id.* ¶¶ 62, 123-124. Although Adobe contends that there can be no actionable dispute
21 concerning the adequacy of Adobe’s security controls because the Agreement expressly provides
22 that no security measure is “100%” effective, Mot. at 14, this disclaimer does not relieve Adobe of
23 the responsibility (also contained in the Agreement) to provide “reasonable” security, *see*
24 Agreement at 4; Compl. ¶ 120.

25 The remaining jurisdictional prerequisites for a declaratory relief claim are met here as
26 well. The dispute over the reasonableness of Adobe’s security controls touches on the parties’ legal
27 relations, and the parties’ legal interests are adverse. *See MedImmune*, 549 U.S. at 127. Plaintiffs
28

1 plausibly allege that they face a substantial risk of future harm if Adobe’s security shortcomings
 2 are not redressed, making this dispute sufficiently real and immediate,¹⁰ and the dispute underlying
 3 Plaintiffs’ declaratory relief claim concerns Adobe’s current security practices, rather than a
 4 hypothetical set of acts or omissions.¹¹ *See id.*

5 Adobe contends that Plaintiffs seek an impermissible advisory opinion, claiming that
 6 Plaintiffs admit that declaratory relief is necessary “only so that users . . . who suffer identity theft
 7 . . . will not have to individually re-litigate the technical issue of Adobe’s security obligations.”
 8 Mot. at 14 (emphasis removed) (citing Compl. ¶ 5). Adobe is correct that declaratory relief claims
 9 brought solely for the purpose of gaining an advantage for future litigation are impermissible. *See*
 10 *Calderon v. Ashmus*, 523 U.S. 740, 747 (1998). However, Plaintiffs are not seeking an advance
 11 ruling on whether Adobe’s security practices in 2013 were reasonable at that time. Rather, the
 12 dispute is over Adobe’s *current* practices. Compl. ¶ 124 (“Plaintiffs . . . seek a declaration [] that
 13 Adobe’s *existing* security measures do not comply with its contractual obligations” (emphasis
 14 added)). Thus, the Court finds that Plaintiffs’ declaratory relief claim does not merely seek an
 15 advisory opinion for use in future breach of contract actions.

16 The Court concludes that Plaintiffs have plausibly alleged that they satisfy the statutory
 17 jurisdictional requirements for obtaining declaratory relief. Adobe is not entitled to dismissal of
 18 Plaintiffs’ claim on this basis.

19
 20
 21 ¹⁰ Adobe contends that Plaintiffs do not allege “any adverse consequences of sufficient immediacy
 22 and reality [] in the absence of their requested judicial declarations.” Mot. at 14 (emphasis
 23 removed). However, Plaintiffs’ complaint specifically alleges that “Adobe’s customers will remain
 24 at risk of attack until the company completely revamps its security practices.” Compl. ¶ 66.
 25 Plaintiffs then substantiate this allegation of threatened harm by listing a number of Adobe’s
 26 allegedly unreasonable security practices, *id.* ¶ 62, and identifying previous instances in which
 27 Adobe has allegedly inadequately responded to security threats, *id.* ¶¶ 43, 55.

28 ¹¹ Adobe resists this conclusion on the grounds that the remedial security measures Plaintiffs
 propose do not take into account the evolving meaning of “reasonable” and are not sufficiently
 specific or definitive because they refer to “industry standards” and similar undefined terms. Reply
 at 6. This is unpersuasive. For one thing, the Court is not bound to adopt the precise wording of any
 potential declaration set forth in a plaintiff’s complaint in deciding how to award declaratory relief,
 and in any event, Adobe’s objections would not prevent the Court from declaring that Adobe’s
 current security practices are unreasonable. Such a decree would constitute “specific relief” that
 would conclusively address the real dispute surrounding the scope of Adobe’s existing contractual
 obligations.

3. Breach of Contract Claim in “Disguise”

Adobe’s third and final challenge to Plaintiffs’ declaratory relief claim is that Plaintiffs are “seeking a declaration that Adobe has breached its contractual obligations” without having alleged all the elements of a breach of contract claim. Mot. at 15. Relying on *Gamble v. GMAC Mortgage Corp.*, No. 08-5532, 2009 WL 400359 (N.D. Cal. Feb. 18, 2009), and *Household Financial Services, Inc. v. Northern Trade Mortgage Corp.*, No. 99-2840, 1999 WL 782072 (N.D. Ill. Sept. 27, 1999), Adobe contends that Plaintiffs’ claim therefore falls outside the scope of the Declaratory Judgment Act. *Id.*

Adobe mischaracterizes Plaintiffs’ declaratory relief claim. In both *Gamble* and *Household Financial*, the plaintiffs sought a judicial decree stating that the defendants had breached their contractual obligations. *Gamble*, 2009 WL 400359, at *2 (“[P]laintiffs want the court to issue a declaratory judgment declaring that defendants breached the forbearance agreements”); *Household Fin.*, 1999 WL 782072, at *3 (“Plaintiff does not request the court to clarify the parties’ rights under the loan purchase agreement. Rather, plaintiff requests a judicial declaration that defendant breached the agreement.”). That is not what Plaintiffs seek here. As discussed above, Plaintiffs seek a declaration clarifying Adobe’s *ongoing* contractual obligation to provide reasonable security. Opp’n at 15; Compl. ¶ 124 (“Plaintiffs . . . seek a declaration [] that Adobe’s *existing* security measures do not comply with its contractual obligations” (emphasis added)). Plaintiffs’ claim thus requests precisely the type of relief that the Declaratory Judgment Act is supposed to provide: a declaration that will prevent future harm from ongoing and future violations before the harm occurs. *See, e.g. Minn. Min. & Mfg. Co. v. Norton Co.*, 929 F.2d 670, 673 (Fed. Cir. 1991) (“In promulgating the Declaratory Judgment Act, Congress intended to prevent avoidable damages from being incurred by a person uncertain of his rights and threatened with damage by delayed adjudication.”). As the Court finds that Plaintiffs are not seeking a declaration that Adobe was in breach of a contract at the time of the 2013 data breach, the Court concludes that Plaintiffs are not required to plead the elements of a breach of contract claim. The Court therefore declines to dismiss Plaintiffs’ declaratory relief claim on this basis.

1 For the foregoing reasons, the Court finds that Plaintiffs have plausibly pleaded that they
2 fulfill both Article III’s standing requirements and the statutory jurisdictional requirements of the
3 Declaratory Judgment Act. The Court also finds that Plaintiffs have plausibly stated a claim for
4 declaratory relief. Accordingly, the Court DENIES Adobe’s Motion to Dismiss Plaintiffs’
5 declaratory relief claim.

6 C. UCL Injunction Claim

7 Plaintiffs’ third cause of action is for injunctive relief under the UCL on behalf of all
8 Plaintiffs (“UCL injunction claim”). *See* Compl. ¶¶ 125-132. The UCL creates a cause of action for
9 business practices that are: (1) unlawful, (2) unfair, or (3) fraudulent. Cal. Bus. & Prof. Code
10 §§ 17200 *et seq.* The UCL’s coverage is “sweeping,” and its standard for wrongful business
11 conduct is “intentionally broad.” *In re First Alliance Mortg. Co.*, 471 F.3d 977, 995 (9th Cir. 2006)
12 (internal quotation marks omitted). Each prong of the UCL provides a separate and distinct theory
13 of liability. *Lozano v. AT & T Wireless Servs., Inc.*, 504 F.3d 718, 731 (9th Cir. 2007). To assert a
14 UCL claim, a private plaintiff must have “suffered injury in fact and . . . lost money or property as
15 a result of the unfair competition.” *Rubio v. Capital One Bank*, 613 F.3d 1195, 1203 (9th Cir.
16 2010) (quoting Cal. Bus. & Prof. Code § 17204). Plaintiffs assert claims under both the “unfair”
17 and “unlawful” prongs of the UCL. Compl. ¶ 126.

18 Adobe seeks dismissal of Plaintiffs’ UCL injunction claim on three grounds. First, Adobe
19 contends that Plaintiffs lack standing to bring this claim. Mot at 16. Second, Adobe contends that
20 Plaintiffs impermissibly seek a contract remedy without bringing a breach of contract claim. *Id.*
21 Finally, Adobe contends that Plaintiffs have failed to allege any conduct that is unfair or unlawful
22 within the meaning of the UCL. *Id.* The Court addresses each of Adobe’s contentions below.

23 1. Standing

24 Adobe argues that, just as with Plaintiffs’ CRA and declaratory relief claims, Plaintiffs lack
25 Article III standing to bring their UCL injunction claim because no Plaintiff has suffered an injury-
26 in-fact. *Id.* For the same reason, Adobe contends that Plaintiffs lack statutory standing to bring a
27 claim under the UCL. *Id.* The Court finds that Plaintiffs have Article III standing to bring their
28

1 UCL injunction claim for the same reasons that Plaintiffs have Article III standing to bring their
2 CRA and declaratory relief claims. *See supra* Part III.A.1; Part III.B.1.

3 Adobe further argues that Plaintiffs lack statutory standing under the UCL. Mot. at 16. In
4 order to establish standing for a UCL claim, plaintiffs must show they personally lost money or
5 property “as a result of the unfair competition.” Cal. Bus. & Prof. Code § 17204; *Kwikset Corp. v.*
6 *Superior Court*, 51 Cal. 4th 310, 330 (2011). “There are innumerable ways in which economic
7 injury from unfair competition may be shown. A plaintiff may (1) surrender in a transaction more,
8 or acquire in a transaction less, than he or she otherwise would have; (2) have a present or future
9 property interest diminished; (3) be deprived of money or property to which he or she has a
10 cognizable claim; or (4) be required to enter into a transaction, costing money or property, that
11 would otherwise have been unnecessary.” *Id.* at 323.

12 Four of the six Plaintiffs allege they personally spent more on Adobe products than they
13 would had they known Adobe was not providing the reasonable security Adobe represented it was
14 providing. *See* Compl. ¶ 79 (“Had Mr. Kar known that Adobe’s security practices were inferior to
15 industry standard security practices, he would not have purchased [a] license online”); *id.* ¶ 84
16 (“Had Ms. Halpain known that Adobe employed substandard security practices, she would not
17 have subscribed to the Creative Cloud service.”); *id.* ¶ 91 (“Had Ms. McGlynn known that Adobe
18 employed substandard security practices, she would not have subscribed to the Creative Cloud
19 Service.”); *id.* ¶¶ 98-99 (“McHenry purchased Adobe Illustrator . . . for approximately \$579.99
20 [He] relied on Adobe’s Privacy Policy and believed that Adobe would provide reasonable
21 security”). Only Plaintiffs Duke and Page do not allege this or any other UCL injury.

22 The Court finds plausible Plaintiffs Kar, Halpain, McGlynn, and McHenry’s allegations
23 that they relied on Adobe’s representations regarding security to their detriment. The parties agree
24 that every Plaintiff was required to accept Adobe’s Privacy Policy before creating an account or
25 providing Adobe with their personal information. Compl. ¶¶ 31-32; Mot. at 3. In that policy,
26 Adobe represented that it would provide reasonable measures to protect customers’ personal
27 identifying and financial information. *See* Mot. at 12. It is also plausible that a company’s
28

1 reasonable security practices reduce the risk of theft of customer’s personal data and thus that a
 2 company’s security practices have economic value. *See Kwikset*, 51 Cal. 4th at 330 (Plaintiffs can
 3 establish UCL standing by alleging they paid more than they actually valued the product); *see also*
 4 *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1072 (N.D. Cal. 2012) (finding UCL
 5 standing was adequately pleaded where plaintiffs claimed they paid more for iPhones than they
 6 would if they had known of defendant’s alleged misrepresentations or omissions).

7 Accordingly, the Court finds that Plaintiffs Kar, Halpain, McGlynn, and McHenry have
 8 plausibly pleaded that they have standing to bring their UCL injunction claim. Plaintiffs Duke and
 9 Page, however, have not, though the Court cannot conclude they would be unable to cure this
 10 deficiency in an amended complaint. Accordingly, the Court GRANTS Adobe’s Motion to Dismiss
 11 Plaintiffs’ UCL injunction claim as to Plaintiffs Duke and Page without prejudice. As to the
 12 remaining Plaintiffs, Adobe is not entitled to dismissal of Plaintiffs’ UCL injunction claim on the
 13 basis of standing.

14 2. Contract Remedy

15 Adobe additionally argues that Plaintiffs’ UCL injunction claim, like Plaintiffs’ declaratory
 16 relief claim, is actually a contract claim in disguise. Mot. at 17. Specifically, Adobe claims that the
 17 UCL injunction claim is, in reality, a claim for specific performance of the Agreement. *Id.*
 18 (“Plaintiffs’ claim . . . is that Adobe should be ordered to ‘honor the terms of its contracts’
 19 Thus, what Plaintiffs seek is the contract remedy of *specific performance*.” (quoting Compl.
 20 ¶ 129)). As specific performance is a contract remedy, Adobe contends that Plaintiffs need to plead
 21 a breach of contract claim in order to seek specific performance. *Id.* (citing *Forever 21, Inc. v.*
 22 *Nat’l Stores Inc.*, No. 12-10807, 2014 WL 722030, at *5 (C.D. Cal. Feb. 24, 2014); *Guidiville*
 23 *Rancheria of Cal. v. United States*, --- F. Supp. 2d ---, 2013 WL 6512788, at *13 (N.D. Cal. Dec
 24 12, 2013)). Plaintiffs have not done so, and thus Adobe contends that Plaintiffs’ UCL injunction
 25 claim fails as a matter of law. *Id.*

26 Plaintiffs acknowledge that they have not pleaded a breach of contract claim. Opp’n at 21.
 27 Nevertheless, Plaintiffs contend that their request for an injunction is just that—a request for an
 28

1 injunction under the UCL, not one for the contract remedy of specific performance. *Id.* As
 2 Plaintiffs are not seeking a contract remedy, Plaintiffs contend they do not need to plead the
 3 elements of breach of contract. *Id.*

4 The Court agrees with Plaintiffs that their request is indeed a request for an injunction
 5 under the UCL, and not one for specific performance. Plaintiffs do not allege that Adobe violated
 6 the UCL solely on the grounds that Adobe failed to “honor the terms of its contracts.” *See* Compl.
 7 ¶¶ 128-131. While Plaintiffs do allege “systematic breach of [] contracts” as one of Adobe’s
 8 allegedly unlawful practices, Plaintiffs also allege that Adobe’s actions are independently unlawful
 9 because they violate the duty California imposes on businesses to reasonably safeguard customers’
 10 data under the CRA. Compl. ¶ 130; *accord* Opp’n at 21 (“Adobe’s duties arose from promises it
 11 made in its contracts and elsewhere, *and from statute.*” (emphasis added)). The Court has already
 12 determined that Plaintiffs have standing to bring claims under this statute. *See supra* Part III.A.
 13 Thus, contrary to Adobe’s assertion, Plaintiffs have alleged a basis for a UCL violation other than
 14 breach of contract. The Court therefore concludes that Plaintiffs’ request is for an injunction to
 15 remedy Adobe’s alleged UCL violations, and not to remedy an unalleged breach of contract.

16 3. Unlawful or Unfair

17 Adobe further challenges Plaintiffs’ UCL injunction claim on the ground that Plaintiffs do
 18 not plead any “unlawful” or “unfair” conduct that violates the UCL. Mot. at 18-19. The Court first
 19 considers Plaintiffs’ “unlawful” allegations, then turns to Plaintiffs’ “unfair” allegations.

20 a. Unlawful

21 The “unlawful” prong of the UCL prohibits “anything that can properly be called a business
 22 practice and that at the same time is forbidden by law.” *Cel-Tech*, 20 Cal. 4th at 180 (internal
 23 quotation marks omitted). By proscribing “any unlawful” business practice, the UCL permits
 24 injured consumers to “borrow” violations of other laws and treat them as unlawful competition that
 25 is independently actionable. *Id.* As predicates for their claim under the UCL’s “unlawful” prong,
 26 Plaintiffs allege that Adobe: (1) violated the CRA, (2) systematically breached contracts, and (3)
 27 “failed to comport with a reasonable standard of care and California public policy” as embodied in
 28

1 a number of California statutes. Compl. ¶ 130 (citing the CRA, the Online Privacy Protection Act
2 (“OPPA”), Cal. Bus. & Prof. Code § 22576, and the Information Practices Act (“IPA”), Cal. Civ.
3 Code §§ 1798 *et seq.*).

4 Adobe argues that none of these allegations are adequate to sustain a UCL claim. As to
5 Plaintiffs’ CRA allegation, Adobe contends that because Plaintiffs lack standing to bring a CRA
6 claim, Plaintiffs similarly lack standing to pursue a UCL claim premised on a violation of the CRA.
7 Mot. at 18. However, the Court has found that Plaintiffs *do* have standing to bring their CRA
8 claim, and thus standing presents no barrier to Plaintiffs’ efforts to base their UCL unlawful claim
9 on Adobe’s alleged violation of the CRA. Accordingly, the Court finds that Plaintiffs have
10 adequately alleged unlawful conduct that may serve as a basis for a claim under the UCL’s
11 unlawful prong, and Adobe is therefore not entitled to dismissal of the UCL unlawful claim on this
12 basis. Because Adobe’s alleged CRA violation is sufficient to sustain Plaintiffs’ UCL unlawful
13 claim, the Court need not address Adobe’s arguments concerning Plaintiffs’ additional allegations
14 of unlawful conduct.

15 **b. Unfair**

16 The “unfair” prong of the UCL creates a cause of action for a business practice that is
17 unfair even if not proscribed by some other law. *Korea Supply Co. v. Lockheed Martin Corp.*, 29
18 Cal. 4th 1134, 1143 (2003). “The UCL does not define the term ‘unfair.’ . . . [And] the proper
19 definition of ‘unfair’ conduct against consumers ‘is currently in flux’ among California courts.”
20 *Davis v. HSBC Bank Nev., N.A.*, 691 F.3d 1152, 1169 (9th Cir. 2012) (citing *Lozano*, 504 F.3d at
21 735). Nevertheless, there are at least two possible tests: (1) the “tethering test,” which requires
22 “that the public policy which is a predicate to a consumer unfair competition action under the
23 ‘unfair’ prong of the UCL must be tethered to specific constitutional, statutory, or regulatory
24 provisions,” and (2) the “balancing test,” which examines whether the challenged business practice
25 is “immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers and
26 requires the court to weigh the utility of the defendant’s conduct against the gravity of the harm to
27
28

1 the alleged victim.”¹² *Drum v. San Fernando Valley Bar Ass’n*, 182 Cal. App. 4th 247, 257 (2010).
 2 As predicates for their claim under the UCL’s “unfair” prong, Plaintiffs allege that Adobe’s
 3 conduct fails the “balancing test” because the conduct was “immoral, unethical, . . . or substantially
 4 injurious” and caused harm that outweighed the conduct’s utility. Compl. ¶ 131. Plaintiffs further
 5 allege that Adobe’s conduct fails the “tethering test” because the conduct violated public policy as
 6 embodied in the CRA, the OPPA, and the IPA. *Id.*

7 Adobe contends that Plaintiffs’ claim under the “balancing test” is “conclusory and
 8 formulaic.” Mot. at 19. Specifically, Adobe claims that Plaintiffs do not allege any injuries
 9 stemming from Adobe’s allegedly unfair conduct and thus that there is no “harm” to balance
 10 against any “utility.” Reply at 9-10. As to the “tethering test,” Adobe contends that Plaintiffs’
 11 allegations fail because Plaintiffs do not allege any violations of the OPPA or the IPA, Mot. at 19,
 12 or any effects that are “comparable to . . . a violation of” those statutes, Reply at 9 (quoting *Cel-*
 13 *Tech*, 20 Cal. 4th at 187).

14 Adobe’s argument that Plaintiffs’ “balancing test” allegations are insufficient is
 15 unpersuasive. Adobe appears to object that Plaintiffs do not allege any injuries resulting from
 16 Adobe’s allegedly unfair conduct in the precise paragraph of the Complaint asserting a claim under
 17 the “balancing test.” Mot. at 19. However, while Plaintiffs are required to plead enough facts in
 18 support of their claims, the pleading standard is not so rigid as to insist that each count repeat every
 19 factual allegation. Rather, the complaint must be specific and clear enough *as a whole* such that the
 20 Court can evaluate the plausibility of each claim and the defendant is placed on notice as to the
 21 basis for the plaintiff’s claims. *See, e.g., McVicar v. Goodman Global, Inc.*, --- F. Supp. 2d ---,
 22 2014 WL 794585, at *7 (C.D. Cal. Feb. 25, 2014) (“[T]he thrust of [defendant’s] argument is
 23

24 ¹² In *Williamson v. Reinalt-Thomas Corp.*, No. 11-3548, 2012 WL 1438812, at *11 (N.D. Cal. Apr.
 25 25, 2012), this Court recognized that the “balancing test” is sometimes construed as two separate
 26 tests. In *Williamson*, this Court noted that some California appellate courts have interpreted the
 27 balancing test to require only that a court “weigh the utility of the defendant’s conduct against the
 28 gravity of the harm to the alleged victim.” *S. Bay Chevrolet v. Gen. Motors Acceptance Corp.*, 72
 Cal. App. 4th 861, 886 (1999). On the other hand, other appellate state courts have applied a
 slightly different version of the balancing test, which mandates that plaintiffs show that a practice
 is “immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers.” *Bardin*
v. Daimlerchrysler Corp., 136 Cal. App. 4th 1255, 1260 (2006).

1 simply to point out that under the section entitled ‘Count One: Violation of [the UCL],’ the
 2 [plaintiffs] do not specifically reference the other sections of the Complaint that identify unlawful
 3 business practices. . . . The UCL does not create such a formalistic pleading requirement.”).
 4 Elsewhere in the Complaint, Plaintiffs allege that Adobe’s conduct placed Plaintiffs at a substantial
 5 risk of future harm and caused Plaintiffs to overpay for Adobe products and services. *See, e.g.,*
 6 Compl. ¶¶ 67-73, 139. The Court has already found that these allegations of injury are sufficient
 7 for Plaintiffs to have standing to bring their UCL injunction claim. *See supra* Part III.C.1. For the
 8 same reasons, the Court finds that Plaintiffs have set forth enough factual allegations of injury to
 9 bring a claim under the “balancing test.”

10 Turning to the “tethering test,” the Court notes that contrary to Adobe’s assertion, Plaintiffs
 11 do not need to plead any direct violations of a statute to bring a claim under the UCL’s unfair
 12 prong. Instead, Plaintiffs need merely to show that the effects of Adobe’s conduct “are comparable
 13 to or the same as a violation of the law, or otherwise significantly threaten[] or harm[]
 14 competition.” *Cel-Tech*, 20 Cal. 4th at 187. Plaintiffs argue that the OPPA, the IPA, and the CRA
 15 collectively reflect California’s public policy of “protecting customer data.” Opp’n at 20. The
 16 Court agrees that California legislative intent is clear on this point, and thus finds that Plaintiffs
 17 have adequately alleged that Adobe’s conduct is “comparable” to a violation of law. *See, e.g.,* Cal.
 18 Civ. Code § 1798.1 (“The Legislature declares that . . . all individuals have a right of privacy in
 19 information pertaining to them. . . . The increasing use of computers . . . has greatly magnified the
 20 potential risk to individual privacy that can occur from the maintenance of personal information.”);
 21 Cal. Civ. Code § 1798.81.5(a) (“It is the intent of the Legislature to ensure that personal
 22 information about California residents is protected.”); Cal. Bus. & Prof. Code § 22578 (explaining
 23 that the Legislature’s intent was to have a uniform policy state-wide regarding privacy policies on
 24 the Internet). Accordingly, the Court concludes that Plaintiffs have pleaded adequate facts to bring
 25 a claim under the “tethering test” of the UCL’s “unfair” prong.

26 In sum, the Court concludes that Plaintiffs Duke and Page have not adequately pleaded that
 27 they have standing to bring a claim under the UCL. The Court therefore GRANTS Adobe’s Motion
 28

1 to Dismiss this claim as to Plaintiffs Duke and Page without prejudice. However, the Court finds
 2 that Plaintiffs Halpain, McGlynn, Kar, and McHenry have adequately pleaded both standing and
 3 the necessary elements to bring their UCL injunction claim. Accordingly, the Court DENIES
 4 Adobe's Motion to Dismiss this claim as to those Plaintiffs.

5 **D. UCL Restitution Claim**

6 Plaintiffs' fourth and final cause of action is for restitution under the UCL on behalf of
 7 purchasers of Adobe's ColdFusion and Creative Cloud products and services ("UCL restitution
 8 claim"). *See* Compl. ¶¶ 133-140. Plaintiffs assert claims under both the "fraudulent" and "unfair"
 9 prongs of the UCL on the basis that Adobe "fail[ed] to disclose that it does not enlist industry
 10 standard security practices." Compl. ¶ 135. Adobe objects to Plaintiffs' UCL restitution claim on
 11 three grounds. First, Adobe contends that the proposed representatives of a restitution class,
 12 Plaintiffs Halpain and McGlynn, lack standing to represent ColdFusion customers as both allege
 13 only that they subscribed to Creative Cloud. Mot. at 20. Second, Adobe contends that Plaintiffs
 14 have not adequately pleaded an omission under the "fraudulent" prong of the UCL. *Id.* Third,
 15 Adobe contends that Plaintiffs have not adequately pleaded a claim under the "unfair" prong of the
 16 UCL. *Id.* at 25.

17 **1. Standing to Bring Restitution Claims for ColdFusion Customers**

18 Some courts reserve the question of whether plaintiffs may assert claims based on products
 19 they did not buy until ruling on a motion for class certification. *See, e.g., Forcellati v. Hyland's,*
 20 *Inc.*, 876 F. Supp. 2d 1155, 1161 (C.D. Cal. 2012); *Cardenas v. NBTY, Inc.*, 870 F. Supp. 2d 984,
 21 992 (E.D. Cal. 2012). Others "hold that a plaintiff may have standing to assert claims for unnamed
 22 class members based on products he or she did not purchase so long as the products and alleged
 23 misrepresentations are substantially similar." *Miller v. Ghirardelli Chocolate Co.*, 912 F. Supp. 2d
 24 861, 869 (N.D. Cal. 2012) (citing cases); *see also, e.g., Colucci v. ZonePerfect Nutrition Co.*, No.
 25 12-2907, 2012 WL 6737800, at *4 (N.D. Cal. Dec. 28, 2012); *Astiana v. Dreyer's Grand Ice*
 26 *Cream, Inc.*, No. 11-2910, 2012 WL 2990766, at *11-13 (N.D. Cal. July 20, 2012). Still other
 27 courts have dismissed claims for lack of standing when the plaintiff did not purchase the product
 28

1 on which the claim is based. *See, e.g., Granfield v. NVIDIA Corp.*, No. 11-5403, 2012 WL
2 2847575, at *6 (N.D. Cal. July 11, 2012) (“[W]hen a plaintiff asserts claims based both on
3 products that she purchased and products that she did not purchase, claims relating to products not
4 purchased must be dismissed for lack of standing.”); *Carrea v. Dreyer’s Grand Ice Cream, Inc.*,
5 No. 10-1044, 2011 WL 159380, at *3 (N.D. Cal. Jan. 10, 2011), *aff’d on other grounds*, 475 F.
6 App’x 113 (9th Cir. 2012).

7 This Court has previously applied the “substantially similar” approach and will do so again
8 here. *E.g., Werdebaugh v. Blue Diamond Growers*, No. 12-2724, 2013 WL 5487236, at *12 (N.D.
9 Cal. Oct. 2, 2013); *Brazil v. Dole Food Co.*, No. 12-1831, 2013 WL 5312418, at *7 (N.D. Cal. Sep
10 23, 2013). Under this approach, both the products themselves and the misrepresentations the
11 plaintiff challenges must be similar, though not identical. In this case, the misrepresentations and
12 omissions at issue are the same for both ColdFusion and Creative Cloud, as all Adobe products are
13 governed by the same privacy policy. *See* Compl. ¶¶ 29-32. Adobe contends, however, that
14 ColdFusion and Creative Cloud are sufficiently dissimilar *as products* that Plaintiffs lack standing
15 to assert claims as to ColdFusion. Drawing from the Complaint, Adobe identifies the following
16 differences between the two products: (1) ColdFusion is licensed-based whereas Creative Cloud is
17 subscription-based; (2) customers use ColdFusion to build dynamic web sites whereas Adobe uses
18 Creative Cloud to sell software subscriptions; and (3) ColdFusion costs up to several thousand
19 dollars per license whereas Creative Cloud plans cost “between \$19.99 and \$79.99” a month. Mot.
20 at 20 n.11 (citing Compl. ¶¶ 19-20). The Court notes, however, that Plaintiff Halpain alleges that
21 she uses Creative Cloud to build websites, Compl. ¶ 89, thus suggesting that both Creative Cloud
22 and ColdFusion can be used for website development. Therefore, assuming the Complaint’s
23 allegations are true, as the Court must on a motion to dismiss, the Court is not persuaded by
24 Adobe’s second-identified difference.

25 The Court finds that the remaining two differences between ColdFusion and Creative Cloud
26 are not significant enough to prevent the products from being “substantially similar” for purposes
27 of the claims alleged here. Plaintiffs’ theory of harm for their UCL restitution claim is that
28

1 ColdFusion and Creative Cloud are “heavily security-dependent” products that Plaintiffs either
 2 would not have purchased or for which Plaintiffs would not have paid as much had Plaintiffs
 3 known the truth about Adobe’s inadequate security practices. Opp’n at 17; Compl. ¶¶ 136-139.
 4 Neither the cost of a product nor whether the product is license- or subscription-based is relevant to
 5 the inquiry here, *i.e.*, whether purchasers of the products valued security, and thus whether they
 6 overpaid for their Adobe products in light of Adobe’s alleged misrepresentations and omissions
 7 regarding security. This distinguishes this case from cases applying the substantially similar
 8 approach in the food mislabeling context, where differences in the products could be expected to
 9 have an impact on whether the customer purchased the product in reliance on the defendant’s
 10 misrepresentations. *See, e.g., Larsen v. Trader Joe’s Co.*, No. 11-5188, 2012 WL 5458396, at *1, 4
 11 (N.D. Cal. June 14, 2012) (plaintiffs lacked standing to challenge label statements on products
 12 plaintiffs did not purchase where products at issue were as disparate as cinnamon rolls, ricotta
 13 cheese, apple juice, and sandwich cookies). Accordingly, the Court concludes that Plaintiffs have
 14 pleaded sufficient facts to establish that Plaintiffs Halpain and McGlynn, the proposed
 15 representatives of a restitution class, have standing to assert claims related to both Creative Cloud
 16 and ColdFusion.

17 2. Fraudulent

18 For an omission to be actionable under the UCL, “the omission must be contrary to a
 19 representation actually made by the defendant, or an omission of a fact the defendant was obliged
 20 to disclose.” *Daugherty v. Am. Honda Motor Co.*, 144 Cal. App. 4th 824, 835 (2006); *see also*
 21 *Berryman v. Merit Prop. Mgmt., Inc.*, 152 Cal. App. 4th 1544, 1557 (2007) (“[A] failure to disclose
 22 a fact one has no affirmative duty to disclose is [not] ‘likely to deceive’ anyone within the meaning
 23 of the UCL.” (quoting *Daugherty*, 144 Cal. App. 4th at 838)). The California Courts of Appeal
 24 have held that there are four circumstances in which a duty to disclose may arise: “(1) when the
 25 defendant is the plaintiff’s fiduciary; (2) when the defendant has exclusive knowledge of material
 26 facts not known or reasonably accessible to the plaintiff; (3) when the defendant actively conceals
 27 a material fact from the plaintiff; [or] (4) when the defendant makes partial representations that are
 28

1 misleading because some other material fact has not been disclosed.” *Collins v. eMachines, Inc.*,
2 202 Cal. App. 4th 249, 255 (2011). “[A] fact is deemed ‘material,’ and obligates an exclusively
3 knowledgeable defendant to disclose it, if a ‘reasonable [consumer]’ would deem it important in
4 determining how to act in the transaction at issue.” *Id.* at 256 (citing *Engalla v. Permanente Med.*
5 *Grp., Inc.*, 15 Cal. 4th 951, 977 (1997)). Plaintiffs claim that Adobe had exclusive knowledge of
6 the fact that its security practices fell short of industry standards, and that this fact was material.
7 Opp’n at 17-18. Accordingly, Plaintiffs claim that Adobe had a duty to disclose this fact, and that
8 Adobe’s failure to do so is an actionable omission under the UCL. *Id.*

9 Adobe does not dispute that facts regarding its security practices are material. Rather,
10 Adobe contends that Adobe did not have exclusive knowledge of its security practices because
11 Adobe’s security shortcomings were widely reported in the press before the 2013 data breach. Mot.
12 at 21-22; Reply at 11-13. Specifically, Adobe notes that its security problems were detailed in
13 articles published by *CNN Money*, the *New York Times*, the *Wall Street Journal*, and *Reuters*,
14 Reply at 12, and further that Plaintiffs knew of these reports, *id.* (noting that the original individual
15 complaints cite some of these reports); see Compl. ¶¶ 42-46 (listing security problems prior to the
16 2013 data breach under the heading “Adobe’s Abysmal Security Record”). Adobe notes that courts
17 in other cases have found that defendants did not have “exclusive knowledge” of the alleged
18 omission when the allegedly omitted fact was widely reported in similarly reputable news sources.
19 Reply at 11-12 (citing *Herron v. Best Buy Co.*, 924 F. Supp. 2d 1161, 1175-76 (E.D. Cal. 2013)
20 (finding that defendants did not have exclusive knowledge of battery testing conditions when those
21 conditions had been reported in *Newsweek*); *Gray v. Toyota Motor Sales, U.S.A.*, No. 08-1690,
22 2012 WL 313703, at *8 (C.D. Cal. Jan. 23, 2012) (finding that defendant did not have exclusive
23 knowledge of discrepancy between EPA estimate of car’s gas mileage and real-world results when
24 discrepancy was reported in *Consumer Reports* and *USA Today*)). Adobe contends that “as a matter
25 of law and logic,” Adobe could not have exclusive knowledge of the fact that it “had not
26 implemented several industry-standard security measures.” *Id.* at 11 (internal quotation marks
27 omitted).

1 The Court is not convinced. It is one thing to have a poor reputation for security in general,
 2 but that does not mean that Adobe's specific security shortcomings were widely known. None of
 3 the press reports Adobe identifies discusses any specific security deficiencies, and Plaintiffs
 4 expressly allege that the extent of Adobe's security shortcomings were revealed only *after* the 2013
 5 data breach. Compl. ¶ 59. Given that prior reports of Adobe's security problems were highly
 6 generic, the Court cannot say that Adobe did not have exclusive knowledge of its failure to
 7 implement industry-standard security measures.¹³ Furthermore, the exact nature of what was in the
 8 public domain regarding Adobe's security practices is a question of fact not properly resolved on a
 9 motion to dismiss.

10 Adobe further argues that even if Plaintiffs identify an actionable omission, Plaintiffs
 11 cannot allege that they relied on that omission, as is required for a claim under the "fraudulent"
 12 prong of the UCL. Mot. at 23 (citing *In re Facebook PPC Adver. Litig.*, No. 09-3043, 2010 WL
 13 3341062, at *9 (N.D. Cal. Aug. 25, 2010)). Adobe reasons that both Halpain and McGlynn could
 14 have cancelled their subscriptions to Creative Cloud upon learning of Adobe's security
 15 deficiencies. Mot. at 24. Neither did so, and indeed, Halpain re-subscribed to Creative Cloud after
 16 her subscription had terminated. *Id.* Adobe argues that Plaintiffs' actions are therefore inconsistent
 17 with their allegations that they would not have subscribed to Creative Cloud had they known of
 18 Adobe's security deficiencies. *Id.* (citing *Noll v. eBay, Inc.*, No. 11-4585, 2013 WL 2384250, at *4
 19 (N.D. Cal. May 30, 2013)).

20 The Court disagrees. Plaintiffs allege that they would not have subscribed to Creative Cloud
 21 in the first instance had they known of Adobe's allegedly unsound security practices. Compl. ¶¶ 84,
 22 91. Having invested time, money, and energy in Creative Cloud, however, Plaintiffs allege that the
 23 costs to switch to another product—which include early cancellation fees, *id.* ¶¶ 88, 93—are now

24
 25 ¹³ Adobe's reliance on *Herron* and *Gray* is misplaced. In both those cases, the press had widely
 26 reported the *exact* omission for which the plaintiffs sought to hold the defendant liable. *See*
 27 *Herron*, 924 F. Supp. 2d at 1175-76 (no actionable omission where both the defendant and the
 28 press had reported the testing conditions used to measure a laptop's battery life); *Gray*, 2012 WL
 313703, at *8 (no actionable omission where press reported that the EPA's gas mileage estimates
 for the Toyota Prius were significantly higher than real-world experience). There is no such
 specificity here.

1 too high to justify abandoning their Creative Cloud subscriptions. *See* Opp'n at 19 (citing Compl.
 2 ¶ 137). This is a plausible allegation. Moreover, a plaintiff need not allege that a product became
 3 totally worthless to her once the defendant's misrepresentation came to light in order to plead
 4 actionable reliance. Rather, it is enough to allege that the product is worth *less* to the plaintiff in
 5 light of the misrepresentation. *See Kwikset*, 51 Cal. 4th at 330 (plaintiff may establish reliance by
 6 alleging that she "paid more than . . . she actually valued the product"). Thus, Plaintiffs need not
 7 have concluded that Creative Cloud is completely worthless, and thus have canceled their
 8 subscriptions, in order to have detrimentally relied on Adobe's alleged misrepresentations or
 9 omissions regarding security.¹⁴ Accordingly, the Court finds that Plaintiffs have not pleaded
 10 themselves out of court by alleging that they did not cancel their Creative Cloud subscriptions upon
 11 learning of Adobe's omissions regarding security.

12 For these reasons, the Court concludes that Plaintiffs have adequately pleaded that Adobe
 13 had a duty to disclose that its security practices were not up to industry standards, that this
 14 omission was material, and that Plaintiffs relied on this omission to their detriment. Thus, Plaintiffs
 15 have adequately pleaded their UCL restitution claim under the UCL's "fraudulent" prong, and
 16 Adobe is not entitled to dismissal of this claim.

17 3. Unfair

18 Plaintiffs also assert two claims under the UCL's "unfair" prong for their UCL restitution
 19 claim. First, Plaintiffs allege that Adobe's competition invested in industry-standard security
 20 practices, and therefore Adobe gained an unfair competitive advantage to the extent that Adobe did
 21 not. Compl. ¶ 138. Plaintiffs contend that this conduct was "unethical, unscrupulous, and
 22
 23

24 ¹⁴ Adobe's authority is not to the contrary. In *Noll*, the plaintiffs alleged that defendant eBay failed
 25 to disclose that listing fees automatically recurred every 30 days. 2013 WL 2384250, at *2.
 26 Critically, the *Noll* plaintiffs did not allege that they would incur any costs, direct or hidden, if they
 27 cancelled their listings. *Id.* Yet the *Noll* plaintiffs continued to pay the listing fees even after they
 28 discovered that the fees recurred automatically. *Id.* Their behavior after discovering the omission
 was therefore exactly the same as their behavior before they knew of the omission, logically
 foreclosing any allegations of reliance. *Id.* at *4. Here, in contrast, Plaintiffs plausibly allege that
 they faced costs to cancelling their subscriptions and to not re-subscribing that they did not face
 when deciding whether to subscribe to Creative Cloud in the first place.

1 substantially injurious.” *Id.* Second, Plaintiffs allege that Adobe’s conduct undermined California
2 public policy as embodied in the OPPA, the IPA, and the CRA. *Id.*

3 Adobe’s objection to these claims again is that Plaintiffs did not include all of the factual
4 allegations supporting these claims in the section of the Complaint that lays out the UCL restitution
5 claim. *See* Mot. at 25; Reply at 15. As previously discussed, *see supra* Part III.C.3.b., the pleading
6 standard does not require that every factual allegation needs to be repeated for every cause of
7 action, *e.g. McVicar*, 2014 WL 794585, at *7. Elsewhere in the Complaint, Plaintiffs identify a
8 number of specific industry-standard security measures that Adobe allegedly did not implement,
9 Compl. ¶ 62, and allege that Adobe’s competitors did invest in these measures, *id.* ¶ 138; *see also*
10 *id.* ¶ 60 (“[C]ompanies like Adobe that do business with major financial institutions or credit card
11 issues must certify that their security measures and protocols are compliant with [an industry
12 standard].”). Plaintiffs therefore plausibly allege that Adobe gained an unfair competitive
13 advantage by not spending money on security the way its competitors did. Plaintiffs also plausibly
14 allege that they were injured by Adobe’s conduct in that they overpaid for Adobe products as a
15 result. *Id.* ¶ 139.

16 Adobe also repeats the argument that Plaintiffs’ “public policy” allegations are flawed
17 because Plaintiffs do not plead violations of the OPPA, the IPA, and the CRA. Mot. at 25. As
18 previously discussed, *see supra* Part III.C.3.b, the “unfair” prong does not require Plaintiffs to
19 plead direct violations of these statutes. Instead, the Court has already found that Plaintiffs
20 plausibly allege that the OPPA, the IPA, and the CRA reflect California’s policy objective of
21 reasonably securing customer data. *See supra* Part III.C.3.b. Plaintiffs further plausibly allege that
22 Adobe’s purported failure to provide industry-standard security undermines that policy objective.
23 The Court therefore finds that Plaintiffs have pleaded with sufficient specificity all the necessary
24 elements of a claim under the UCL’s “unfair” prong for their UCL restitution claim, and Adobe is
25 not entitled to dismissal of the claim on that basis.

26 For the foregoing reasons, the Court DENIES Adobe’s Motion to Dismiss Plaintiffs’ UCL
27 restitution claim.

United States District Court
For the Northern District of California

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

IV. CONCLUSION

For the reasons discussed above, the Court:

- 1. GRANTS Adobe’s Motion to Dismiss Plaintiffs’ CRA claim for violations of Section 1798.82 without prejudice;
- 2. GRANTS Adobe’s Motion to Dismiss Plaintiffs’ UCL injunction claim as to Plaintiffs Duke and Page without prejudice; and
- 3. DENIES the remainder of Adobe’s Motion to Dismiss.

Should Plaintiffs elect to file a Second Amended Complaint curing the deficiencies identified herein, Plaintiffs shall do so within thirty days of the date of this Order. Failure to meet the thirty-day deadline to file an amended complaint or failure to cure the deficiencies identified in this Order will result in a dismissal with prejudice. Plaintiffs may not add new causes of actions or parties without leave of the Court or stipulation of the parties pursuant to Federal Rule of Civil Procedure 15.

IT IS SO ORDERED.

Dated: September 4, 2014



 LUCY H. KOH
 United States District Judge