

United States District Court
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

IN RE: YAHOO! INC. CUSTOMER DATA
SECURITY BREACH LITIGATION

Case No. 16-MD-02752-LHK

**ORDER GRANTING IN PART AND
DENYING IN PART MOTION TO
DISMISS**

Re: Dkt. No. 94

Plaintiffs Kimberly Heines, Hashmatullah Essar, Paul Dugas, Matthew Ridolfo, Deana Ridolfo, Rajesh Garg, Scarleth Robles, Maria Corso, Jose Abitbol, Yaniv Rivlin, Mali Granot, and Brian Neff (collectively, “Plaintiffs”) bring a putative class action against Defendant Yahoo! Inc. (“Yahoo”). Plaintiff Brian Neff also brings a putative class action against Defendant Aabaco Small Business, LLC (“Aabaco”) (collectively with Yahoo, “Defendants”).

Before the Court is Defendants’ motion to dismiss Plaintiffs’ Consolidated Class Action Complaint (“CCAC”). ECF No. 94 (“Mot.”). Having considered the parties’ submissions, the relevant law, and the record in this case, the Court hereby GRANTS in part and DENIES in part the motion to dismiss.

I. BACKGROUND

1 **A. Factual Background**

2 Defendant Yahoo was founded in 1994 and has since grown into a source for internet
3 searches, email, shopping, news and many other internet services. CCAC ¶ 24. One of Yahoo’s
4 most important services is Yahoo Mail, a free email service. *Id.* ¶ 25. Plaintiffs allege that
5 “[m]any users have built their digital identities around Yahoo Mail, using the service for
6 everything from their bank and stock trading accounts to photo albums and even medical
7 information.” *Id.*

8 Yahoo also offers online services for small business, including website hosting and email
9 services (hereinafter, “Small Business Services”). *Id.* ¶ 29. Users must pay for Small Business
10 Services, and users are required to provide credit or debit card information for automatic monthly
11 payments for Small Business Services. *Id.* Prior to November 2015, Yahoo provided these
12 services through a division called Yahoo Small Business. *Id.* “Since November 2015, Yahoo has
13 provided its small business services through its wholly owned subsidiary Aabaco.” *Id.*

14 Plaintiffs allege that in order to obtain email services and Small Business Services from
15 Defendants, users are required to provide personal identification information (“PII”) to Defendant.
16 This PII includes the user’s name, email address, birth date, gender, ZIP code, occupation,
17 industry, and personal interests.¹ CCAC ¶¶ 1, 32. For some Yahoo accounts, including the small
18 business accounts, users are required to submit additional PII, including credit or debit card
19 numbers and other financial information. *Id.* ¶ 32.

20 In addition to the PII that Plaintiffs submitted directly to Defendants, Plaintiffs also allege
21 that users used their Yahoo email accounts to send and receive a variety of personal information.
22 Each named Plaintiff alleges that he or she included sensitive PII in the content of his or her
23 Yahoo emails. The individual allegations of the named Plaintiffs, including allegations regarding
24 the personal information that these named Plaintiffs included in their Yahoo email accounts, are
25 discussed further below.

26 _____
27 ¹ The CCAC also mentions other Yahoo services, including Yahoo Fantasy Wallet and Yahoo
28 Messenger. *See* CCAC ¶¶ 24–28. However, the CCAC does not allege that any named Plaintiff
used these services, and accordingly the Court does not discuss these services.

1. Earlier 2012 Data Breach Putting Yahoo on Notice of Data Security Issues

1 Plaintiffs allege that Defendants have a long history of data security failures that should
 2 have put Defendants on notice of the need to enhance their data security. For example, although
 3 the Federal Trade Commission found as early as 2003 that “SQL injection attacks” were a known
 4 and preventable data security threat, “[i]n 2012, Yahoo admitted that more than 450,000 user
 5 accounts were compromised through an SQL injection attack—with the passwords simply stored
 6 in plain text.” *Id.* ¶ 47–48. Plaintiffs allege that according to news stories at the time, “[s]ecurity
 7 experts were befuddled . . . as to why a company as large as Yahoo would fail to cryptographically
 8 store the passwords in its database. Instead, [the passwords] were left in plain text, which means a
 9 hacker could easily read them.” *Id.*

10 According to Plaintiffs, the 2012 hackers intended the 2012 attack as a wake-up call, and
 11 the hackers left a message stating “We hope that the parties responsible for managing the security
 12 of this subdomain will take this as a wake-up call, and not as a threat . . . There have been many
 13 security holes exploited in Web servers belonging to Yahoo! Inc. that have caused far greater
 14 damage than our disclosure. Please do not take them lightly.” *Id.* ¶ 49. However, despite this
 15 warning, Plaintiffs allege that “Yahoo’s internal culture actively discouraged emphasis on data
 16 security.” *Id.* ¶ 50. Plaintiffs allege that “former Yahoo security staffers interviewed later told
 17 Reuters that requests made by Yahoo’s security team for new tools and features such as
 18 strengthened cryptography protections were, at times, rejected on the grounds that the requests
 19 would cost too much money, were too complicated, or were simply too low a priority.” *Id.* ¶ 50.

2. Three Data Breaches at Issue in the Instant Case

20 The instant lawsuit involves three data breaches that occurred between 2013 and 2016.
 21 According to Plaintiffs, Defendants represented to users that users’ accounts with Defendants were
 22 secure. For example, Yahoo’s website stated that “protecting our systems and our users’
 23 information is paramount to ensuring Yahoo users enjoy a secure user experience and maintaining
 24 our users’ trust” and that “[w]e have physical, electronic, and procedural safeguards that comply
 25 with federal regulations to protect personal information about you.” *Id.* ¶ 34. Similarly, Aabaco’s
 26
 27
 28

1 website stated that “[w]e have physical, electronic, and procedural safeguards that comply with
2 federal regulations to protect your Personal Information.” *Id.* ¶ 35. Nonetheless, despite these
3 representations, Plaintiffs allege that Defendants did not use appropriate safeguards to protect
4 users’ PII and that Plaintiffs’ PII was thus exposed to hackers who infiltrated Defendants’ systems.
5 Specifically, Plaintiffs allege three separate data breaches: a breach that occurred in 2013, a breach
6 that occurred in 2014, and a “forged cookie breach” that occurred in 2015 and 2016. The Court
7 refers to these breaches collectively as the “Data Breaches.” The Court discusses each below.

8 **a. The 2013 Breach**

9 The first breach occurred in August 2013 (“2013 Breach”). *Id.* ¶ 56. At that time, hackers
10 gained access to more than one billion Yahoo accounts and stole users’ Yahoo login, country
11 code, recovery e-mail, date of birth, hashed passwords, cell phone numbers, and zip codes. *Id.*
12 Plaintiffs allege that this 2013 Breach was particularly egregious “given the fact that 1 billion
13 accounts were compromised, when there are only 3 billion people with Internet access in the
14 world.” *Id.* ¶ 59 (internal quotation marks and brackets omitted).

15 Significantly, the 2013 Breach also gave hackers access to the contents of users’ emails,
16 and thus exposed any PII or other sensitive information that users included in the contents of their
17 emails. *Id.* Plaintiffs allege that users used their Yahoo emails for a variety of personal and
18 financial transactions, and thus that Yahoo email accounts contained “records involving credit
19 cards, retail accounts, banking, account passwords, IRS documents, and social security numbers
20 from transactions conducted by email, in addition to other confidential and sensitive information
21 contained therein.” *Id.* ¶ 1.

22 Yahoo did not disclose the fact of the 2013 Breach until December 14, 2016, over three
23 years after the 2013 Breach occurred in August 2013. *Id.* ¶ 78. Plaintiffs allege that the 2013
24 Breach occurred because Yahoo did not timely move away from an outdated encryption
25 technology known as MD5. *Id.* ¶ 53. According to Plaintiffs, it was widely recognized in the data
26 security industry long before the 2013 Breach that MD5 was “cryptographically broken and
27 unsuitable for further use.” *Id.* ¶ 55. Nevertheless, Yahoo did not begin to upgrade from MD5
28

1 until the summer of 2013. *Id.* ¶¶ 54–55. Plaintiffs allege, however, that Yahoo’s move from MD5
2 in the summer of 2013 was too late to prevent the 2013 Breach. *Id.* ¶¶ 54–55.

3 **b. The 2014 Breach**

4 The second breach occurred in late 2014 (“2014 Breach”). Plaintiffs allege that “the 2014
5 breach began with a ‘spear phishing’ email campaign sent to upper-level Yahoo employees. One
6 or more of these employees fell for the bait, and Yahoo’s data security was so lax, that this action
7 was enough to hand over the proverbial keys to the kingdom.” *Id.* ¶ 91. Through this attack,
8 hackers gained access to at least 500 million Yahoo user accounts. *Id.* ¶ 62. Many of the accounts
9 breached in the 2014 Breach were accounts that had previously been breached in the 2013 Breach.
10 *Id.* ¶ 63. In its motion to dismiss, Yahoo states that it received evidence from law enforcement
11 that the criminal intruders responsible for the 2013 Breach were unrelated to the perpetrators of
12 the 2014 Breach. *See Mot.* at 19.²

13 According to Plaintiffs, in August 2016, hackers posted for sale on the dark web the
14 personal information of 200,000,000 Yahoo users. *Id.* ¶ 70. Plaintiffs also allege that “a
15 geographically dispersed hacking group based in Eastern Europe managed to sell copies of the
16 database to three buyers for \$300,000 apiece months before Yahoo disclosed the 2014 Breach.”
17 *Id.* ¶ 71.

18 Plaintiffs allege that Yahoo knew about the 2014 Breach as it was happening, but that
19 Yahoo did not publicly disclose the existence of the 2014 Breach until September 22, 2016,
20 approximately two years later. Plaintiffs allege that Yahoo’s announcement of the 2014 Breach
21 “came just two months after Yahoo announced Verizon’s plan to acquire its operating assets, and
22 just weeks after Yahoo reported to the SEC that it knew of no incidents of unauthorized access of
23 personal data that might adversely affect the potential acquisition.” *Id.* ¶ 73. Significantly,
24 Plaintiffs allege that Yahoo delayed notifying users or the public about the 2014 Breach while
25 “Yahoo solicited offers to buy the company. Reportedly, Yahoo wanted the offers in by April 19,

26 _____
27 ² For citations to the parties’ briefs for the instant motion, the Court cites to the page numbers
28 electronically generated at the top of each page by the Court’s ECF docket management system.

1 2016,” and thus waited to disclose the breach until September 2016. *Id.* ¶ 69.

2 Plaintiffs also allege that “[b]y intentionally failing to disclose the breach in a timely
3 manner as required by law, Yahoo misled consumers into continuing to sign up for Yahoo services
4 and products, thus providing Yahoo a continuing income stream and a better chance of finalizing a
5 sale of the company to Verizon.” *Id.* In the September 22, 2016 announcement of the 2014
6 Breach, Yahoo stated that the affected “account information may have included names, email
7 addresses, telephone numbers, dates of birth, hashed passwords (the vast majority with bcrypt)
8 and, in some cases, encrypted or unencrypted security questions and answers.” *Id.* ¶ 73.

9 Plaintiffs allege that Yahoo’s claim that it had not known about the 2014 Breach for two
10 years was “met with immediate skepticism.” *Id.* ¶ 74. Indeed, in a recent 10-K filing with the
11 SEC, Yahoo revealed that an independent investigation determined that Yahoo had
12 contemporaneous knowledge of the 2014 Breach, yet failed to properly investigate and analyze the
13 breach, due in part to “failures in communication, management, inquiry and internal reporting”
14 that led to a “lack of proper comprehension and handling” of the 2014 Breach. *Id.* ¶ 4.

15 **c. The Forged Cookie Breach**

16 The third data breach occurred in 2015 and 2016 (“Forged Cookie Breach”). According to
17 the CCAC, the attackers in the Forged Cookie Breach used forged cookies to access Yahoo users’
18 accounts. “Cookies” are files that Yahoo places on users’ computers to store login information so
19 that users do not need to reenter login information every time the users access their accounts. *Id.* ¶
20 67. By forging these cookies, hackers were able to access Yahoo accounts without needing a
21 password to the accounts. *Id.* ¶ 68. Moreover, by forging cookies, hackers were able to remain
22 logged on to accounts for long periods of time. *Id.* ¶ 68.

23 According to Plaintiffs, the attackers in the Forged Cookie Breach are “presumed to be the
24 same parties involved in the 2014 Breach.” *Id.* Specifically, Plaintiffs allege that “the 2014
25 Breach and Forged Cookie Breach have since been attributed to two Russian FSB agents, a
26 Russian hacker, and a Canadian hacker.” *Id.* ¶ 90. Plaintiffs allege that in a recent 10-K filing
27 with the SEC, Yahoo disclosed that an independent committee of Yahoo’s Board of Directors had

1 determined that Yahoo’s information security team knew, at a minimum, about the Forged Cookie
 2 Breach as it was happening, “but took no real action in the face of that knowledge.” *Id.* ¶ 86.
 3 Instead, Plaintiffs allege, Yahoo “quietly divulged” the existence of the Forged Cookie Breach in
 4 Yahoo’s 10-Q filing with the SEC filed on November 9, 2016 and did not begin notifying users
 5 about the Forged Cookie Breach until February 2017. *Id.* ¶ 80–81.

6 **3. Allegations of Individual Named Plaintiffs**

7 The CCAC is brought by eleven named Plaintiffs on behalf of four putative classes. The
 8 Court briefly discusses the allegations of these individual named Plaintiffs below.

9 **a. Named Plaintiffs Representing the United States Class**

10 Plaintiffs Kimberley Heines, Hasmatullah Essar, Paul Dugas, Matthew Ridolfo, Deana
 11 Ridolfo, and Rajesh Garg (“United States Plaintiffs”) assert claims on behalf of the putative
 12 United States Class, which consists of all Yahoo account holders in the United States whose
 13 accounts were compromised in any of the Data Breaches. CCAC ¶¶ 10–14, 105.

14 Plaintiff Kimberley Heines (“Heines”), a resident of California, alleges that she used her
 15 Yahoo email account in conjunction with Direct Express, which is the service through which
 16 Heines receives her Social Security, and thus her Yahoo email account “included information
 17 relating to her account with Direct Express.” *Id.* ¶ 10. In 2015, Heines discovered that her
 18 monthly Social Security benefits had been stolen from her Direct Express account and used to
 19 purchase gift cards. *Id.* As a result, Heines fell behind on her bills, and she paid late fees as a
 20 result. *Id.* After the theft, Heines began receiving debt collection calls for debts she herself had
 21 not incurred, and she saw unfamiliar debts appearing on her credit report, which harmed her credit
 22 score. *Id.* Heines alleges that she has spent over 40 hours dealing with the consequences of the
 23 identity theft. *Id.*

24 Plaintiff Hasmatullah Essar (“Essar”), a resident of Colorado, used two free Yahoo email
 25 accounts. *Id.* ¶ 11. Essar used these accounts “for all of his personal, financial, and business
 26 needs” including receiving bank statements, applying for jobs, and securing a mortgage. *Id.* Essar
 27 began receiving “phishing emails from a credit card company purporting to be affiliated with

1 American Express, asking him to follow a link to log-in to his ‘Serve’ account,” which Essar did
2 not own. *Id.* After Essar was notified of the 2014 Breach, Essar signed up for and has paid
3 \$35.98 per month for LifeLock credit monitoring service. *Id.* In February 2017, “an unauthorized
4 person fraudulently filed a tax return under his Social Security Number,” and in March 2017 he
5 was denied credit and had freezes placed on his credit. *Id.*

6 Plaintiff Paul Dugas (“Dugas”), a resident of California, used four Yahoo email accounts
7 “for his banking, investment accounts, business emails, and personal emails.” *Id.* ¶ 12. In April of
8 2016, Dugas was unable to file his personal tax returns because a tax return had already been filed
9 under his Social Security Number. *Id.* As a result, “both of his college-aged daughters missed
10 deadlines to submit” their financial aid applications, and accordingly Dugas was forced to pay
11 \$9,000 in educational expenses that he otherwise would not have had to pay. *Id.* Moreover,
12 Dugas has also experienced numerous fraudulent charges on his credit cards, he has had to replace
13 his credit cards, and he has had to pay money to three different credit bureaus to freeze his
14 accounts. *Id.*

15 Plaintiffs Matthew Ridolfo and Deana Ridolfo, a married couple, are residents of New
16 Jersey. *Id.* ¶ 13. They both “used their Yahoo accounts for nearly twenty years, for general
17 banking, credit card management and communications, a mortgage refinance, and communication
18 with friends and family.” *Id.* Both Matthew and Deana Ridolfo experienced numerous instances
19 of credit card fraud as a result of the Data Breaches. *Id.* Specifically, eleven credit card or bank
20 accounts were opened or attempted to be opened in Matthew Ridolfo’s name, and at least eleven
21 credit card accounts were opened or attempted to be opened in Deana Ridolfo’s name. *Id.* The
22 Ridolfos experienced fraudulent charges on their credit cards. *Id.* The Ridolfos eventually
23 purchased and enrolled in LifeLock to help monitor their credit and finances, and they each pay
24 \$30.00 per month for these services. *Id.* Nonetheless, as late as January 31, 2017, an
25 unauthorized person opened an additional credit card in Matthew Ridolfo’s name. *Id.*

26 Plaintiff Rajesh Garg (“Garg”), a citizen of Illinois, “used his Yahoo account for banking,
27 investment accounts, business emails, banking, credit card, healthcare, social security, and for

1 friends and family.” *Id.* ¶ 14. Garg suffered significant embarrassment when unauthorized and
2 inappropriate emails were sent on his behalf to his business and personal contacts. *Id.*

3 **b. Named Plaintiffs Representing the Israel Class**

4 Plaintiffs Yaniv Rivlin and Mali Granot (“Israel Plaintiffs”) assert claims on behalf of the
5 putative Israel Class, which consists of all Yahoo account holders in Israel whose accounts were
6 compromised in any of the Data Breaches. *Id.* ¶¶ 15–16, 105.

7 Plaintiff Yaniv Rivlin (“Rivlin”), a resident of Tel Aviv, Israel, used his Yahoo email
8 account “mainly for personal purposes, including banking, friends and family, credit card
9 statements, and social security administration.” *Id.* ¶ 15. Rivlin also pays Yahoo \$20.00 per
10 month for an email forwarding service and keeps a credit card on file with Yahoo to pay for the
11 service. *Id.* After being notified that his account had been breached, Rivlin has noticed an
12 increase in spam and unsolicited advertisements, and Rivlin has spent considerable time changing
13 many user names and passwords on many accounts to prevent fraud. *Id.*

14 Plaintiff Mali Granot (“Granot”), a resident of Raanana, Israel, uses her Yahoo email
15 account “to correspond with family, friends and school.” *Id.* ¶ 16. Granot was unexpectedly
16 locked out of her account and, when she regained access, Granot received numerous unsolicited
17 chat requests and other unsolicited services. *Id.*

18 **c. Named Plaintiffs Representing Australia, Venezuela, and Spain Class**

19 Plaintiffs Scarleth Robles, Mara Corso, and Jose Abitbol (“Australia, Venezuela, and Spain
20 Plaintiffs”) assert claims on behalf of the putative Australia, Venezuela, and Spain Class, which
21 consists of all Yahoo account holders in Australia, Venezuela, or Spain whose accounts were
22 compromised in any of the Data Breaches. *Id.* ¶¶ 17–19, 105.

23 Plaintiff Scarleth Robles (“Robles”), a resident of Venezuela, uses her Yahoo account to
24 “advise[] entrepreneurs on business ventures and ideas and requests that potential clients send
25 their entrepreneurial and business proposals to her Yahoo email address.” *Id.* ¶ 17. Around
26 September 2016, Robles noticed that business proposals disappeared from her email account and
27 unidentified persons “stole business ideas from her email account.” *Id.* As a result, Robles alleges

1 that she lost “approximately ten clients” from her business. *Id.*

2 Plaintiff Maria Corso (“Corso”), a resident of Clearview, South Australia, used her Yahoo
3 email account to “send sensitive information, including financial documents, her tax security
4 number, work history, and medical information.” *Id.* ¶ 18. Corso was locked out of her account
5 without warning, and after contacting Yahoo customer service, Corso was told that “Russian
6 hackers tried over 60 times to gain access to her Yahoo email account.” *Id.* Corso also purchased
7 security protection and continues to pay an annual fee of \$150 for that service. *Id.*

8 Plaintiff Jose Abitbol (“Abitbol”) is a resident of New York but a citizen of Spain. *Id.* ¶
9 19. Abitbol alleges that his “Yahoo email account contains sensitive and confidential information,
10 including information about his bank accounts, business, investment accounts, credit cards,
11 personal matters, and social security number.” *Id.* After obtaining Abitbol’s “bank account
12 number through his Yahoo email account,” an unknown person made at least two fraudulent wire
13 transfer requests for a total of \$50,000. *Id.*

14 **d. Named Plaintiff Representing the Small Business Users Class**

15 Plaintiff Brian Neff (“Small Business Users Plaintiff” or “Neff”) asserts claims on behalf
16 of a putative Small Business Users Class, which consists of all Yahoo business account holders in
17 the United States whose accounts were compromised in any of the Data Breaches. *Id.* ¶¶ 20, 105.
18 Plaintiff Neff, a resident of Texas, “contracted with Yahoo for two services, Yahoo! Web Hosting
19 for www.TheInsuranceSuite.com and Yahoo! Business Email, for which he has paid Yahoo
20 \$13.94 every month” *Id.* ¶ 20. Neff has also used Yahoo and Aabaco’s web hosting services
21 “in connection with another 54 websites, paying anywhere from \$3.94 to \$15.94 per month for
22 each website.” *Id.* In May 2015, Neff incurred fraudulent charges on two of his credit cards, both
23 of which were on file with Yahoo to pay for the services described above. *Id.* Additionally, a
24 credit card was fraudulently opened in Neff’s name. Neff has spent “significant time and incurred
25 expenses mitigating the harm to him from these security breaches and identity theft.” *Id.* Neff
26 also “intends to migrate his insurance agency website, www.TheInsuranceSuite.com, to a more
27 secure provider,” which Neff alleges will require significant expenses. *Id.*

B. Procedural History

1 After the 2014 Breach was announced on September 22, 2016, a number of lawsuits were
2 filed against Defendants. These lawsuits generally alleged that Yahoo failed to adequately protect
3 its users' accounts, that Yahoo failed to disclose its inadequate data security practices, and that
4 Yahoo failed to timely notify users of the data breach.

5 In late 2016, Plaintiffs in several lawsuits moved to centralize pretrial proceedings in a
6 single judicial district. *See* 28 U.S.C. § 1407(a) (“When civil actions involving one or more
7 common questions of fact are pending in different districts, such actions may be transferred to any
8 district for coordinated or consolidated pretrial proceedings.”). On December 7, 2016, the Judicial
9 Panel on Multidistrict Litigation (“JPML”) issued a transfer order selecting the undersigned judge
10 as the transferee court for “coordinated or consolidated pretrial proceedings” in the multidistrict
11 litigation (“MDL”) arising out of the 2014 Breach. *See* ECF No. 1 at 1–3.

12 On December 14, 2016, one week after the JPML issued the transfer order for cases arising
13 from the 2014 Breach, Yahoo announced the existence of the 2013 Breach. Plaintiffs in several
14 lawsuits that had been filed regarding the 2014 Data Breach then amended their complaints to
15 include claims regarding the 2013 Breach. Additionally, more lawsuits were filed in the Northern
16 District of California regarding the 2013 Breach and the 2014 Breach. Again, these lawsuits
17 generally alleged that Yahoo failed to adequately protect its users' accounts, that Yahoo failed to
18 disclose its inadequate data security practices, and that Yahoo failed to timely notify users of the
19 data breach.

20 This Court found that claims regarding the 2013 Breach were related under Civil Local
21 Rule 3-12 to claims regarding the 2014 Breach, and therefore all lawsuits in the Northern District
22 of California regarding the 2014 Breach were reassigned to the undersigned judge. ECF Nos. 7, 9,
23 30, 40, 64. Additionally, the JPML issued a conditional transfer order transferring one case
24 regarding the 2013 Breach, *Baker v. Yahoo*, 17-CV-00135, to the undersigned judge. ECF No. 33.

25 On February 9, 2017, the Court held a hearing to appoint Lead Plaintiffs' Counsel. ECF
26 No. 56. Following this hearing, the Court issued an order appointing a Plaintiffs' Executive
27

1 Committee. ECF No. 58. At a case management conference on March 2, 2017, the Court ordered
 2 the Plaintiffs’ Executive Committee to file a consolidated amended complaint by April 12, 2017.
 3 ECF No. 68. Plaintiffs then filed the instant Consolidated Class Action Complaint (“CCAC”) on
 4 April 12, 2017. ECF No. 80. The CCAC asserts one federal statutory claim, five California
 5 statutory claims, and seven California common law claims. *Id.* At a further case management
 6 conference on May 4, 2017, the Court determined that because there is a “limited number of
 7 claims . . . , many of those claims contain overlapping elements, and the case involves only two
 8 defendants, one of which is a subsidiary of the other,” the first motion to dismiss should “proceed
 9 without phasing.” ECF No. 89.

10 On May 22, 2017, Defendants filed the instant motion to dismiss. ECF No. 94 (“Mot.”).
 11 The same day, Defendants filed a request for judicial notice in connection with their motion to
 12 dismiss. ECF No. 95. On June 30, 2017, Plaintiffs filed an opposition to Defendants’ motion to
 13 dismiss, ECF No. 117 (“Opp.”), and a response to Defendants’ request for judicial notice, ECF
 14 No. 118. On August 1, 2017, Defendants filed a reply in support of their motion to dismiss, ECF
 15 No. 121 (“Reply”), and a reply in support of their request for judicial notice, ECF No. 122. On
 16 August 10, 2017, Defendants filed a notice of errata to their reply in support of the motion to
 17 dismiss. ECF No. 124. On August 15, 2017, Plaintiffs filed an administrative motion for leave to
 18 file a sur-reply, ECF No. 126, and a statement of recent decision pursuant to Civil Local Rule 7-
 19 3(d)(2), ECF No. 127.

20 **II. LEGAL STANDARD**

21 **A. Motion to Dismiss Under Rule 12(b)(6)**

22 Pursuant to Federal Rule of Civil Procedure 12(b)(6), a defendant may move to dismiss an
 23 action for failure to allege “enough facts to state a claim to relief that is plausible on its face.” *Bell*
 24 *Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). “A claim has facial plausibility when the
 25 plaintiff pleads factual content that allows the court to draw the reasonable inference that the
 26 defendant is liable for the misconduct alleged. The plausibility standard is not akin to a
 27

1 ‘probability requirement,’ but it asks for more than a sheer possibility that a defendant has acted
2 unlawfully.” *Ashcroft v. Iqbal*, 566 U.S. 662, 678 (2009) (internal citation omitted).

3 For purposes of ruling on a Rule 12(b)(6) motion, the Court “accept[s] factual allegations
4 in the complaint as true and construe[s] the pleadings in the light most favorable to the nonmoving
5 party.” *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir.
6 2008). However, a court need not accept as true allegations contradicted by judicially noticeable
7 facts, *Shwarz v. United States*, 234 F.3d 428, 435 (9th Cir. 2000), and a “court may look beyond
8 the plaintiff’s complaint to matters of public record” without converting the Rule 12(b)(6) motion
9 into one for summary judgment, *Shaw v. Hahn*, 56 F.3d 1028, 1029 n.1 (9th Cir. 2011). Mere
10 “conclusory allegations of law and unwarranted inferences are insufficient to defeat a motion to
11 dismiss.” *Adams v. Johnson*, 355 F.3d 1179, 1183 (9th Cir. 2004).

12 **B. Leave to Amend**

13 If the court concludes that a motion to dismiss should be granted, it must then decide
14 whether to grant leave to amend. Under Rule 15(a) of the Federal Rules of Civil Procedure, leave
15 to amend “shall be freely given when justice so requires,” bearing in mind “the underlying purpose
16 of Rule 15 . . . [is] to facilitate decision on the merits, rather than on the pleadings or
17 technicalities.” *Lopez*, 203 F.3d at 1127 (citation omitted). Nonetheless, a district court may deny
18 leave to amend a complaint due to “undue delay, bad faith or dilatory motive on the part of the
19 movant, repeated failure to cure deficiencies by amendments previously allowed, undue prejudice
20 to the opposing party by virtue of allowance of the amendment, [and] futility of amendment.” *See*
21 *Leadsinger, Inc. v. BMG Music Publ’g*, 512 F.3d 522, 532 (9th Cir. 2008) (alteration in original).

22 **III. REQUEST FOR JUDICIAL NOTICE**

23 The Court first addresses Defendants’ request for judicial notice. ECF No. 94. The Court
24 may take judicial notice of matters that are either “generally known within the trial court’s
25 territorial jurisdiction” or “can be accurately and readily determined from sources whose accuracy
26 cannot reasonably be questioned.” Fed. R. Evid. 201(b). Public records, including judgments and
27 other publicly filed documents, are proper subjects of judicial notice. *See, e.g., United States v.*

1 *Black*, 482 F.3d 1035, 1041 (9th Cir. 2007) (“[Courts] may take notice of proceedings in other
2 courts, both within and without the federal judicial system, if those proceedings have a direct
3 relation to matters at issue.”); *Rothman v. Gregor*, 220 F.3d 81, 92 (2d Cir. 2000) (taking judicial
4 notice of a filed complaint as a public record).

5 However, to the extent any facts in documents subject to judicial notice are subject to
6 reasonable dispute, the Court will not take judicial notice of those facts. *See Lee v. City of L.A.*,
7 250 F.3d 668, 689 (9th Cir. 2001) (“A court may take judicial notice of matters of public
8 record . . . But a court may not take judicial notice of a fact that is subject to reasonable dispute.”)
9 (internal quotation marks omitted), *overruled on other grounds by Galbraith v. Cty. of Santa*
10 *Clara*, 307 F.3d 1119 (9th Cir. 2002).

11 Defendants request judicial notice of the following documents:

12 Ex. A: “Security at Yahoo” subpage within Yahoo’s “Privacy Center,”

13 <https://policies.yahoo.com/us/en/yahoo/privacy/topics/security/index.htm>; last accessed:

14 May 18, 2017;

15 Ex. B: Australia Universal Terms of Service, “Yahoo7 Terms of Service,”

16 <https://policies.yahoo.com/au/en/yahoo/terms/utos/index.htm>; last accessed: May 19, 2017;

17 Ex. C: Additional Terms of Service, “Yahoo Communications Terms,”

18 <https://policies.yahoo.com/xw/en/yahoo/terms/product-atos/comms/index.htm>; last

19 accessed: May 19, 2017;

20 Ex. D: Venezuela Universal Terms of Service, “Condiciones del Servicio,”

21 <https://policies.yahoo.com/e2/es/yahoo/terms/utos/index.htm>; last accessed: May 19, 2017;

22 Ex. E: Yahoo Press Release, “An Important Message to Yahoo Users on Security,” dated Sept. 22,

23 2016, <https://investor.yahoo.net/releasedetail.cfm?releaseid=990570>; last accessed: May

24 19, 2017;

25 Ex. F: Yahoo Press Release, “Important Security Information for Yahoo Users,” dated Dec. 14,

26 2016, <https://investor.yahoo.net/ReleaseDetail.cfm?releaseid=1004285>; last accessed: May

27 18, 2017;

- 1 Ex. G: Yahoo! Inc., Annual Report (Form 10-K) (Mar. 1, 2017);
- 2 Ex. H: Yahoo! Inc., Quarterly Report (Form 10-Q) (May 9, 2017);
- 3 Ex. I: Internal Revenue Service Taxpayer Guide to Identity Theft, dated Apr. 18, 2017,
- 4 <https://www.irs.gov/uac/taxpayer-guide-to-identity-theft>; last accessed: May 18, 2017;
- 5 Ex. J: Department of Justice Press Release, “U.S. Charges Russian FSB Officers and Their
- 6 Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts,” dated Mar.
- 7 15, 2017, [https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-](https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions)
- 8 [their-criminal-conspirators-hacking-yahoo-and-millions](https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions); last accessed: May 18, 2017;
- 9 Ex. K: Remarks of Acting Assistant Attorney General for National Security Mary B. McCord,
- 10 “Acting Assistant Attorney General Mary B. McCord Delivers Remarks at Press
- 11 Conference Announcing Charges Against Russian FSB Officers and Their Criminal
- 12 Conspirators for Hacking Yahoo,” dated Mar. 15, 2017,
- 13 [https://www.justice.gov/opa/speech/acting-assistant-attorney-general-mary-b-](https://www.justice.gov/opa/speech/acting-assistant-attorney-general-mary-b-mccord-delivers-remarks-press-conference)
- 14 [mccord-delivers-remarks-press-conference](https://www.justice.gov/opa/speech/acting-assistant-attorney-general-mary-b-mccord-delivers-remarks-press-conference); last accessed: May 18, 2017;
- 15 Ex. L: Second Amended Class Action Complaint, *Dugas v. Starwood Hotels & Resorts*
- 16 *Worldwide, Inc.*, S.D. Cal. Case No. 3:16-CV-00014, Dkt. No. 31;
- 17 Ex. M: Legislative Counsel’s Digest for Senate Bill 46;
- 18 Ex. N: California Assembly, Committee on Judiciary, Analysis of Senate Bill 46;
- 19 Ex. O: Privacy Rights Clearinghouse Letter to Senator Corbett in Support of Senate Bill 46, dated
- 20 Apr. 16, 2013;
- 21 Ex. P: California Assembly, Committee on Appropriations, Analysis of Senate Bill 46;
- 22 Ex. Q: California Assembly, Judiciary Committee, Mandatory Information Worksheet for Senate
- 23 Bill 46.

24 These documents fall into five categories: (1) Documents referenced in the complaint

25 (Exhibits A–G); (2) Securities and Exchange Commission Filings (Exhibits G–H); (3) Information

26 on government websites (Exhibits I–K); (4) Court filings (Exhibit L); and (5) Legislative history

27 documents (Exhibits M–Q).

1 In Plaintiffs' response to Defendants' request for judicial notice, Plaintiffs state that they
2 do not object to judicial notice of Exhibits A through G (documents referenced in the complaint),
3 or Exhibits L through Q (court filings and legislative history documents). ECF No. 118 at 2–4.
4 The Court agrees that these documents are proper subjects of judicial notice. *See United States v.*
5 *Ritchie*, 342 F.3d 903, 908 (9th Cir. 2003) (“Even if a document is not attached to a complaint, it
6 may be incorporated by reference into a complaint if the plaintiff refers extensively to the
7 document or the document forms the basis of the plaintiff’s claim.”); *Reyn’s Pasta Bella, LLC v.*
8 *Visa USA, Inc.*, 442 F.3d 741, 746 n.6 (9th Cir. 2006) (holding that a court “may take judicial
9 notice of court filings and other matters of public record.”); *Anderson v. Holder*, 673 F.3d 1089,
10 1094 n.1 (9th Cir. 2012) (“Legislative history is properly a subject of judicial notice.”). Therefore,
11 the Court GRANTS Defendants’ unopposed request for judicial notice of Exhibits A through G
12 and Exhibits L through Q.

13 As to Exhibits H through K, Plaintiffs concede that SEC filings (Exhibit H) and
14 information on government websites (Exhibits I–K) are proper subjects of judicial notice. Ex. 118
15 at 2–3. However, Plaintiffs state that these documents contain disputed facts that are not proper
16 subjects of judicial notice. Particularly, with respect to Exhibits I through K, Plaintiffs state that
17 “[b]y excerpting specific self-serving statements, rather than referencing the documents as a
18 whole, Defendants suggest that the references are being used to prove the truth of the cited
19 ‘facts.’” *Id.* at 3.

20 However, as discussed above, a court may take judicial notice of a document without
21 taking judicial notice of reasonably disputed facts contained in the document. *See Lee*, 250 F.3d at
22 689 (“A court may take judicial notice of matters of public record . . . But a court may not take
23 judicial notice of a fact that is subject to reasonable dispute.”). As both parties concede, both SEC
24 filings and documents on government websites are proper subjects of judicial notice. *See Michery*
25 *v. Ford Motor Co.*, 650 F. App’x 338, 341 n.2 (9th Cir. 2016) (taking judicial notice of the
26 existence of documents on a government website); *Dreiling v. Am. Exp. Co.*, 458 F.3d 942, 946
27 n.2 (9th Cir. 2006) (holding that “SEC filings” are “subject to judicial notice.”). Thus, the Court

1 GRANTS Defendants’ request for judicial notice of Exhibits H through K, “not for the truth of the
2 facts recited therein, but for the existence of the opinion, which is not subject to reasonable dispute
3 over its authenticity.” *Lee*, 250 F.3d at 690. Because Plaintiffs dispute facts contained within
4 Exhibits H through K, the Court does not take judicial notice of any facts in these documents. The
5 Court next turns to address the substance of Defendants’ motion to dismiss the CCAC.

6 **IV. DISCUSSION**

7 As set forth above, Plaintiffs Kimberley Heines, Hasmatullah Essar, Paul Dugas, Matthew
8 Ridolfo, Deana Ridolfo, and Rajesh Garg (“United States Plaintiffs”) assert claims on behalf of
9 the putative United States Class, which consists of all Yahoo account holders in the United States
10 whose accounts were compromised in any of the Data Breaches. CCAC ¶¶ 10–14, 105.

11 Plaintiffs Yaniv Rivlin and Mali Granot (“Israel Plaintiffs”) assert claims on behalf of the
12 putative Israel Class, which consists of all Yahoo account holders in Israel whose accounts were
13 compromised in any of the Data Breaches. *Id.* ¶¶ 15–16, 105.

14 Plaintiffs Scarleth Robles, Mara Corso, and Jose Abitbol (“Australia, Venezuela, and Spain
15 Plaintiffs”) assert claims on behalf of the putative Australia, Venezuela, and Spain Class, which
16 consists of all Yahoo account holders in Australia, Venezuela, or Spain whose accounts were
17 compromised in any of the Data Breaches. *Id.* ¶¶ 17–19, 105.

18 Plaintiff Brian Neff (“Small Business Users Plaintiff”) asserts claims on behalf of a
19 putative Small Business Users Class, which consists of all Yahoo business account holders in the
20 United States whose accounts were compromised in any of the Data Breaches. *Id.* ¶ 20, 105.

21 The CCAC asserts one federal statutory claim, five California statutory claims, and seven
22 California common law claims on behalf of the four putative classes. Specifically, the CCAC
23 asserts (1) a claim under the California Unfair Competition Law (“UCL”) on behalf of the United
24 States Class and the Israel Class; (2) a claim under the California Consumer Legal Remedies Act
25 (“CLRA”) on behalf of the United States Class and the Israel Class; (3) a claim under the
26 California Customer Records Act (“CRA”) on behalf of the United States Class and the Israel
27 Class; (4) a claim under the federal Stored Communications Act on behalf of the United States

1 Class and the Israel Class; (5) a claim under the California Online Privacy Protection Act on
 2 behalf of the United States Class and the Israel Class; (6) a claim for breach of express contract on
 3 behalf of the United States Class, the Israel Class, and the Small Business Users Class; (7) a claim
 4 for breach of implied contract on behalf of the United States Class, the Israel Class, and the Small
 5 Business Users Class; (8) a claim for breach of the implied covenant of good faith and fair dealing
 6 on behalf of the United States Class, the Israel Class, and the Small Business Users Class; (9) a
 7 claim for fraudulent inducement on behalf of the Small Business Users Class; (10) a claim for
 8 negligent misrepresentation on behalf of the Small Business Users Class; (11) a claim under the
 9 UCL on behalf of the Small Business Users Class; (12) a claim for negligence on behalf of the
 10 Australia, Venezuela, and Spain Class; and (13) a claim for declaratory relief on behalf of all
 11 classes. *Id.* ¶¶ 126–234. All of these claims relate to three data breaches: the 2013 Breach, the
 12 2014 Breach, and the Forged Cookie Breach (collectively, “Data Breaches”).

13 Defendants move to dismiss Plaintiffs’ CCAC in its entirety. First, Defendants argue that
 14 Plaintiffs have not established that they have Article III standing to assert any of their claims.
 15 Next, Defendants raise particular objections to each of Plaintiffs’ thirteen causes of action.

16 The Court first considers Defendants’ arguments regarding Article III standing and then
 17 considers Defendants’ challenges to each of Plaintiffs’ causes of action in turn.

18 **A. Article III Standing**

19 Defendants first move to dismiss the CCAC in its entirety because, according to
 20 Defendants, Plaintiffs lack Article III standing to sue. Article III standing to sue requires that (1)
 21 the plaintiff suffered an injury in fact, i.e., “an invasion of a legally protected interest which is (a)
 22 concrete and particularized, and (b) actual or imminent, not conjectural or hypothetical”; (2) the
 23 injury is “‘fairly traceable’ to the challenged conduct,” and (3) the injury is “likely” to be
 24 “redressed by a favorable decision.” *Lujan v. Def. of Wildlife*, 504 U.S. 555, 560–61 (1992). “The
 25 party invoking federal jurisdiction bears the burden of establishing these elements . . . with the
 26 manner and degree of evidence required at the successive stages of litigation.” *Id.* at 561. At the
 27 pleading stage, “[g]eneral allegations” of injury may suffice. *Id.*

1 Defendants contend that Plaintiffs lack Article III standing because Plaintiffs cannot
2 establish “injury in fact” and because Plaintiffs cannot establish that their injury is “fairly
3 traceable” to the actions of Defendants. *See* Mot. at 20–25. The Court addresses these arguments
4 in turn.

5 **1. Injury In Fact**

6 Defendants argue that Plaintiffs lack Article III standing because Plaintiffs have not
7 suffered an injury in fact that is concrete and particularized. *See* Mot. at 21. In a class action,
8 named plaintiffs representing a class “must allege and show that they personally have been
9 injured, not that injury has been suffered by other, unidentified members of the class to which they
10 belong and which they purport to represent.” *Warth v. Seldin*, 422 U.S. 490, 502 (1975). “[I]f
11 none of the named plaintiffs purporting to represent a class establishes the requisite of a case or
12 controversy with the defendants, none may seek relief on behalf of himself or any other member
13 of the class.” *O’Shea v. Littleton*, 414 U.S. 488, 494 (1974).

14 According to Defendants, named Plaintiffs have not suffered an injury in fact because
15 Plaintiffs allege only vague and unspecified harms, such as the loss of “unspecified information”
16 and emails. Moreover, Defendants argue that Plaintiffs’ other allegations of injury are speculative,
17 and that any monetary injuries suffered by Plaintiffs have been reimbursed. Plaintiffs, by contrast,
18 argue that all Plaintiffs have suffered concrete harms from the Data Breaches, and that several
19 courts have found these harms sufficient to establish injury in fact in similar data breach cases.
20 Specifically, Plaintiffs contend that all Plaintiffs have suffered harm in the form of (1) risk of
21 future identity theft; and (2) loss of value of their PII. *See* Opp. at 15–18. In addition, Plaintiffs
22 contend that several Plaintiffs—although not all Plaintiffs—have experienced additional injuries
23 such as harm from identity theft, consequential out of pocket expenses, and loss of benefit of the
24 bargain. *See id.*

25 For the reasons discussed below, the Court agrees with Plaintiffs that Plaintiffs have
26 adequately alleged injury in fact. The Court first discusses the two injuries that all Plaintiffs allege
27 that they have suffered: (1) the risk of future identity theft, and (2) the loss of value of their PII.

1 The Court then briefly addresses the additional harms suffered by some, although not all,
2 Plaintiffs.

3 **a. Risk of Future Identity Theft**

4 Plaintiffs argue that they have all suffered an injury in fact because Plaintiffs all have
5 suffered an increased risk of future identity theft as a result of the Data Breaches. The Court
6 agrees with Plaintiffs. In *In re Adobe Systems, Inc. Privacy Litigation*, 66 F. Supp. 3d 1197,
7 1214–15 (N.D. Cal. 2014), this Court held that plaintiffs whose PII was exposed during a data
8 breach of Adobe’s servers had standing to sue Adobe for the data breach, even though the
9 plaintiffs’ personal information had not yet been misused by the hackers. In *Adobe*, the plaintiffs
10 alleged that Adobe’s servers were hacked and that the hackers spent “several weeks collecting
11 names, usernames, passwords, email addresses, phone numbers, mailing addresses, and credit card
12 numbers and expiration dates.” *Id.* at 1214. The *Adobe* plaintiffs alleged that their “personal
13 information was among the information taken during the breach,” and that “[s]ome of the stolen
14 data ha[d] already surfaced on the Internet.” *Id.* The Court held that the plaintiffs’ allegations
15 were sufficient “to establish Article III injury-in-fact at the pleadings stage” because the plaintiffs
16 adequately alleged an “imminent” threat that their personal information would be misused by the
17 hackers. *Id.* at 1215.

18 Several other courts have also found that similar allegations of future harm suffice to
19 establish Article III standing at the motion to dismiss stage. For example, in *Krottner v. Starbucks*
20 *Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010), the Ninth Circuit addressed for the first time “whether
21 an increased risk of identity theft constitutes an injury-in-fact.” The Ninth Circuit held that
22 because the plaintiffs “alleged a credible threat of real and immediate harm stemming from the
23 theft of a laptop containing their unencrypted personal data,” the plaintiffs “sufficiently alleged an
24 injury-in-fact for purposes of Article III standing.” *Id.* at 1143.

25 Furthermore, in *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015),
26 the Seventh Circuit cited *Adobe* with approval and held that “[l]ike the Adobe plaintiffs, the
27 Neiman Marcus customers should not have to wait until hackers commit identity theft or credit-

1 card fraud in order to give the class standing, because there is an ‘objectively reasonable
2 likelihood’ that such an injury will occur.” *See also Lewert v. P.F. Chang’s China Bistro, Inc.*,
3 819 F.3d 963, 967 (7th Cir. 2016) (holding that the plaintiffs had established Article III standing
4 based on “the increased risk of fraudulent charges and identity theft they face because their data
5 has already been stolen.”). Similarly, in *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App’x 384,
6 388 (6th Cir. 2016), the Sixth Circuit held that allegations of a risk of future harm were sufficient
7 for Article III standing and noted that “[w]here a data breach targets personal information, a
8 reasonable inference can be drawn that the hackers will use the victims’ data for the fraudulent
9 purposes alleged in Plaintiffs’ complaints.”

10 Plaintiffs’ allegations here are substantially similar to the plaintiffs’ allegations in *Adobe*
11 and other cases finding Article III standing based on the risk of future identity theft. Plaintiffs
12 allege that in the 2013 Breach and the 2014 Breach, “hackers stole the names, email addresses,
13 telephone numbers, birth dates, passwords, and security questions of Yahoo account holders.”
14 CCAC ¶ 1. As a result, hackers gained “access to the email contents of all breached Yahoo
15 accounts.” *Id.* Moreover, in the Forged Cookie Breach, the hackers were able to forge
16 authentication cookies and thus “remain logged into the hacked [email] accounts for weeks or
17 indefinitely.” *Id.* ¶ 68.

18 Plaintiffs allege that, as a result of the Data Breaches, hackers were able to access the
19 contents of Plaintiffs’ email accounts, “and thus any private information contained within those
20 emails, such as financial communications and records involving credit cards.” *Id.* ¶ 1. Indeed,
21 Plaintiffs allege that they used their Yahoo email accounts in connection with numerous personal
22 financial transactions, including receiving Social Security payments, maintaining investment
23 accounts, and filing income tax returns. *See, e.g. id.* ¶¶ 1, 10–14. Like the plaintiffs in *Adobe*,
24 Plaintiffs here allege that their personal information was among the information taken during the
25 Data Breaches. *See id.*; *see also id.* ¶ 1. Further, like the plaintiffs in *Adobe*, Plaintiffs here allege
26 that the stolen data has appeared on the dark web, and has indeed remained for sale on the dark
27 web “as late as March 17, 2017.” *Id.* ¶ 84; *Remijas*, 794 F.3d at 694 (“[O]nce stolen data have

1 been sold or posted on the Web, fraudulent use of that information may continue for years.”).

2 In these circumstances, Plaintiffs have alleged a “credible threat of real and immediate
3 harm” stemming from the data breaches. *Krottner*, 628 F.3d at 1143. There is no dispute that
4 Plaintiffs’ Yahoo accounts were hacked. “Presumably, the purpose of the hack is, sooner or later,
5 to . . . assume those consumers’ identities” or to misuse Plaintiffs’ PII in other ways. *Remijas*, 794
6 F.3d at 693. Indeed, as discussed below, several United States Plaintiffs allege that their stolen PII
7 has *already* been misused by identity thieves, and they have experienced concrete harms as a
8 result. *See infra* Part III.B.c.i.

9 Accordingly, as the Court found in *Adobe*, the Court finds that Plaintiffs have sufficiently
10 alleged “a concrete and imminent threat of future harm suffic[ient] to establish Article III injury-
11 in-fact at the pleadings stage.” *See Adobe*, 66 F. Supp. 3d 1197, 1215.

12 **b. Loss of Value of PII**

13 In addition, Plaintiffs also argue that all Plaintiffs have suffered an injury in fact because
14 the Data Breaches caused all Plaintiffs to suffer a loss of value of their PII as a result of the Data
15 Breaches. *See Opp.* at 17. Again, the Court agrees with Plaintiffs. As the Court explained in *In*
16 *re Anthem, Inc. Data Breach Litigation* (“*Anthem IP*”), 2016 WL 3029783, at *14 (N.D. Cal. May
17 17, 2016), “the Ninth Circuit and a number of district courts have approved” allegations of
18 damages arising from the loss of value of PII. For example, in *In re Facebook Privacy Litigation*,
19 72 F. App’x 494, 494 (9th Cir. 2014), the Ninth Circuit found that the plaintiffs plausibly alleged
20 that they experienced harm where the plaintiffs’ personal information was disclosed in a data
21 breach, and the plaintiffs “los[t] the sales value of th[eir] [personal] information” as a result.
22 Similarly, in *Anthem II*, this Court found that the plaintiffs plausibly alleged injury from the loss
23 of value of their PII where the plaintiffs alleged that their PII was disclosed in a data breach, and
24 that plaintiffs’ PII was subsequently sold on the black market by hackers. *Anthem II*, 2016 WL
25 3029783, at *14–15; *see also Svenson v. Google, Inc.*, 2015 WL 1503429, at *5 (N.D. Cal. Apr. 1,
26 2015) (“Svenson’s allegations of diminution in value of her personal information are sufficient to
27 show contract damages for pleading purposes.”).

1 Plaintiffs allege here that “hackers stole the names, email addresses, telephone numbers,
2 birth dates, passwords, and security questions of Yahoo account holders.” CCAC ¶ 1. Plaintiffs
3 allege that this PII is highly valuable to Defendants because Defendants use this information for
4 “targeted advertising.” *Id.* ¶ 36. Moreover, Plaintiffs allege that this PII is “highly valuable to
5 identity thieves,” and that hackers have sold this PII on the “dark web.” *Id.* ¶ 41. Plaintiffs’
6 CCAC includes several examples of hackers selling PII from Yahoo accounts on the dark web
7 following the Data Breaches. *See, e.g.*, ¶ 70. For example, “[i]n August 2016, a hacker
8 identifying himself or herself as ‘peace_of_mind’ posted for sale on the dark web the PII from 200
9 million Yahoo accounts.” *Id.* As recently as March 17, 2017, stolen information from the Data
10 Breaches “was still for sale on underground hacker forums.” *Id.* ¶ 84. Specifically, the CCAC
11 contains screenshots of hackers selling documents labeled as “Yahoo, 100K, email: pass,
12 decrypted,” and “Yahoo, 5,737,977, decrypted, complete.” *Id.* Plaintiffs allege that this PII is
13 particularly valuable because hackers can use this information, and in many cases *have* used this
14 information, to “gain[] access to the email contents of all breached Yahoo accounts and thus any
15 private information contained within those emails.” *Id.* ¶ 1. Plaintiffs allege that, as a result of
16 their valuable PII being for sale on the dark web, Plaintiffs have lost the value of their PII. *See,*
17 *e.g., id.* ¶¶ 135, 145.

18 Accordingly, as the Court found in *Anthem II*, Plaintiffs’ allegations that their PII is a
19 valuable commodity, that a market exists for Plaintiffs’ PII, that Plaintiffs’ PII is being sold by
20 hackers on the dark web, and that Plaintiffs have lost the value of their PII as a result, are
21 sufficient to plausibly allege injury arising from the Data Breaches. *Anthem II*, 2016 WL
22 3029783, at *15–16 (finding plaintiff plausibly alleged injury where plaintiffs alleged that their
23 PII was a valuable commodity to identity thieves, that an economic market existed for the PII, and
24 that the value of Plaintiffs’ PII decreased as a result of the data breach).

25 c. Additional Harms

26 As set forth above, the Court finds that all Plaintiffs have suffered injury in fact in the form
27 of (1) the risk of future identity theft; and (2) loss of value of their PII. In addition, the Court also

1 finds that individual Plaintiffs, though not all Plaintiffs, have alleged additional injuries in fact as a
 2 result of the Data Breaches. Specifically, some individual Plaintiffs have also alleged (1) that their
 3 stolen PII has already been misused by identity thieves; (2) that they have paid out of pocket
 4 mitigation expenses; and (3) loss of benefit of the bargain. The Court briefly discusses these
 5 additional injuries below.

6 **i. Plaintiffs who Allege their Stolen PII has Already been Misused**

7 First, several United States Plaintiffs allege that their stolen PII has *already* been misused
 8 by identity thieves and that they have experienced concrete harms as a result. For example,
 9 Plaintiffs Essar and Dugas allege that they used their Yahoo email accounts to conduct their
 10 personal finances, and that their Social Security numbers were stolen from their Yahoo email
 11 accounts as a result of the Data Breaches. *See, e.g.*, CCAC ¶¶ 11–12. Dugas alleges that a
 12 fraudulent tax return was filed under his Social Security number and that he was not able to timely
 13 file his own taxes as a result. *Id.* ¶ 12. Because Dugas could not file his own tax return, Dugas
 14 was unable to timely file a financial aid application for his daughters. *Id.* This resulted in Dugas
 15 needing to pay an additional \$9,000 in tuition expenses that he would not otherwise have had to
 16 pay. *Id.*

17 Similarly, Plaintiffs Matthew and Deana Ridolfo allege that they used their Yahoo email
 18 account to manage their personal finances, that their credit card information was stolen from their
 19 Yahoo email accounts in the Data Breaches, and that unauthorized credit card accounts were
 20 subsequently opened in their names. *Id.* ¶ 13. The Ridolofos allege that at least \$900.00 in
 21 unauthorized charges were made in their names. *Id.*

22 Further, Plaintiff Heines alleges that she used her Yahoo email account in connection with
 23 her Social Security Disability benefits, that this information was accessed in the Data Breaches,
 24 and that her Social Security Disability benefits were stolen from her Social Security Disability
 25 benefits account. *Id.* ¶ 10. As a result, Heines alleges that she was unable to pay her bills, and
 26 that she incurred late fees as a result. *Id.* ¶ 10.

27 The Court finds that these allegations are sufficient to allege injury in fact arising from the

1 Data Breaches. *See In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d at 1215 (reasoning that
 2 plaintiffs would clearly have suffered a sufficient injury in fact if the plaintiffs “could allege that
 3 their stolen personal information had already been misused”). Indeed, Defendants do not appear
 4 to contest that harms from misuse of personal data are generally sufficient to confer Article III
 5 standing. Defendants argue that here, however, Plaintiffs have failed to adequately allege Article
 6 III standing because the CCAC does not allege that the fees and charges discussed above went
 7 “unreimbursed.” *See Mot.* at 22. Defendants’ argument is not persuasive. Plaintiffs Essar,
 8 Dugas, Mathew Ridolfo, Deana Ridolfo, and Heines do not allege that the expenses discussed
 9 above *were* reimbursed. *See CCAC ¶¶* 10–14. On a motion to dismiss, the Court must take
 10 Plaintiffs’ factual allegations as true and make all reasonable inferences in Plaintiffs’ favor. Thus,
 11 at this stage of the proceedings, the Court cannot assume that Plaintiffs have been compensated for
 12 the fraudulent charges and resulting fees that Plaintiffs allegedly incurred.

13 Defendants cite *Whalen v. Michaels Stores, Inc.*, 2017 WL 1556116, at *2 (2d Cir. May 2,
 14 2017), in support of Defendants’ argument that Plaintiffs lack Article III standing, even though
 15 Plaintiffs allege that their personal information has already been misused. However, Defendants’
 16 reliance on *Whalen* is not persuasive. First, that case is an unpublished summary order from the
 17 Second Circuit, and it is accordingly not binding on this Court and indeed not binding in the
 18 Second Circuit itself. *See id.* (stating that rulings by summary order do not have precedential
 19 effect). Second, the facts alleged in *Whalen* are readily distinguishable from the instant case. The
 20 plaintiff in *Whalen* alleged that her credit card information was stolen in a data breach, and that
 21 her credit card was subsequently “physically presented for payment” in Ecuador on two occasions.
 22 *Id.* at *1. However, the plaintiff in *Whalen* “cancelled her card,” and she did “not allege that any
 23 fraudulent charges were actually incurred on the card” or that “she was in any way liable on
 24 account of these presentations” of her credit card in Ecuador. *Id.* at *1. The Second Circuit
 25 affirmed the district court’s dismissal of the complaint for lack of Article III standing because
 26 *Whalen* never alleged that fraudulent charges were actually incurred on her credit card, she never
 27 alleged a plausible threat of future fraud “because her stolen credit card was promptly cancelled,”

1 and Whalen did not allege that any other information—such as her birth date or Social Security
 2 number—was taken in the breach. *Id.* Moreover, Whalen did not allege “any time or effort that
 3 she herself has spent monitoring her credit.” *Id.* Thus, the Second Circuit held that Whalen did
 4 not adequately allege that the data breach caused Whalen to suffer any injury that was concrete
 5 and particularized. *Id.*

6 Here, unlike the Plaintiff in *Whalen*, Plaintiffs Essar, Dugas, Matthew Ridolfo, Deana
 7 Ridolfo, and Heines have each alleged more than simply that their credit card was “presented for
 8 payment,” without further allegations of identity theft or harm. *Id.* at 2. As set forth above,
 9 Plaintiffs Essar, Dugas, Matthew Ridolfo, Deana Ridolfo, and Heines allege that hackers obtained
 10 their Yahoo user names and passwords, dates of birth, credit and debit card account information,
 11 and/or Social Security number as a result of the Data Breaches, and that hackers used this
 12 information to steal benefits and/or to make a variety of fraudulent credit card charges and/or
 13 fraudulent tax filings in their names. *See, e.g.*, CCAC ¶ 1 (alleging hackers “stole the names,
 14 email addresses, telephone numbers, birth dates, passwords, and security questions of Yahoo
 15 account holders, in addition to all of the “private information contained within those emails, such
 16 as financial communications and records involving credit cards” and “social security numbers”);
 17 *id.* ¶ 10 (alleging hackers accessed and stole Heines Social Security Disability benefits); *id.* ¶¶ 11–
 18 12 (alleging hackers accessed Essar and Dugas’s Social Security Numbers and filed fraudulent tax
 19 returns under their Social Security Numbers, causing Essar and Dugas to experience harm).
 20 Further, Plaintiffs Essar, Dugas, Matthew Ridolfo, Deana Ridolfo, and Heines allege several
 21 consequential fees resulting from these fraudulent charges and filings, and allege that they were
 22 required to spend significant time and effort monitoring these charges and mitigating their fall out.
 23 *See, e.g.*, CCAC ¶ 1, 10 (alleging Heines incurred late charges because she could not pay her bills
 24 as a result of hackers stealing her Social Security Disability benefits, and that she spent over 40
 25 hours managing the consequences of her identity being stolen); *id.* ¶ 12 (alleging that Dugas used
 26 his Yahoo account for his tax returns, that hackers accessed his account and subsequently filed a
 27 fraudulent tax return under Dugas’s Social Security number, and that Dugas faced additional costs

1 and tax return problems as a result of the breach).

2 Thus, the alleged information stolen in this case, and the alleged harm that resulted, is far
 3 more significant than the information and harm alleged in *Whalen*, where the plaintiff alleged only
 4 that her credit card information was stolen and subsequently “presented for payment,” but no
 5 fraudulent charges were incurred before the credit card was promptly cancelled. *See Whalen*,
 6 2017 WL 1556116, at *2. Accordingly, the Court finds that Plaintiffs Essar, Dugas, Matthew
 7 Ridolfo, Deana Ridolfo, and Heines—who each allege that their stolen personal information has
 8 already been misused in the data breach—have adequately alleged injury in fact. *See In re Adobe*
 9 *Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d at 1215 (reasoning that plaintiffs would clearly have
 10 suffered a sufficient injury in fact if the plaintiffs “could allege that their stolen personal
 11 information had already been misused”).

12 **ii. Plaintiffs Who Have Paid Out-of-Pocket Mitigation Expenses**

13 Second, several Plaintiffs allege that, as a result of the Data Breaches, Plaintiffs have been
 14 required to spend money to monitor their credit and prevent future identity theft. Specifically,
 15 Plaintiff Essar alleges that his personal information was exposed during the Data Breaches and
 16 that he “signed up for and paid (and continues to pay) \$35.98 per month for LifeLock credit
 17 monitoring service” to “limit the damage done to his credit and identity.” CCAC ¶ 11. The
 18 Ridolfos also allege that they each pay \$30.00 a month for LifeLock. *Id.* ¶ 13. Similarly, Plaintiff
 19 Corso alleges that she continues to pay an annual fee of \$150 for account security protection after
 20 her personal information was exposed in the Data Breaches. *Id.* ¶ 18.

21 The Court finds that these allegations of out-of-pocket mitigation expenses are also
 22 sufficient to allege injury in fact arising from the Data Breaches. In other data breach cases,
 23 district courts have held that similar out-of-pocket mitigation expenses are sufficient to allege
 24 Article III injury in fact. *See, e.g., In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d at 1216
 25 (finding costs incurred to mitigate future identity theft sufficient to constitute injury in fact);
 26 *Walters v. Kimpton Hotel & Rest. Grp., LLC*, 2017 WL 1398660, at *1 (N.D. Cal. Apr. 13, 2017)
 27 (finding plaintiffs’ allegations regarding efforts to “monitor his credit” following identity theft to

1 be sufficient to demonstrate injury in fact). Indeed, Defendants’ motion to dismiss does not
2 address these out-of-pocket mitigation expenses, and Defendants do not argue that out-of-pocket
3 mitigation expenses are insufficient to allege injury in fact. *See* Mot. at 21–22. Accordingly, for
4 the reasons set forth above, the Court finds that Plaintiffs Essar, Matthew Ridolfo, Deana Ridolfo,
5 and Corso—who each allege that they incurred costs to mitigate future identity theft as a direct
6 result of the Data Breaches—have alleged an additional injury in fact.

7 **iii. Benefit of the Bargain Losses**

8 Finally, Small Business Users Plaintiff Neff alleges that he has suffered injury in fact from
9 lost benefit of the bargain. As a user of Defendants’ Small Business Services, Neff “has paid
10 Yahoo \$13.94 each month” since September 2009. CCAC ¶ 20. Neff uses Yahoo’s Small
11 Business Services to host Neff’s online insurance agency business. *Id.* Neff alleges that
12 Defendants represented to members of the putative Small Business Users Class that Defendants’
13 Small Business Services were “secure.” *Id.* ¶ 198. Neff alleges that he “would not have agreed to
14 utilize and pay for the small business services and turn over [his] PII” had Neff known that
15 Defendants’ Small Business Services “were not as secure as represented or secure by any
16 standard.” *Id.* ¶ 199. Accordingly, Neff alleges that he has suffered harm because Neff has paid
17 Defendants monthly fees for a product that Neff did not ultimately receive: “secure small business
18 services.” *Id.* ¶ 203.

19 The Court finds that Neff’s allegations are sufficient to allege “benefit of the bargain”
20 losses as a result of the Data Breaches, which courts in this district and elsewhere have found are
21 sufficient to allege an injury in fact for purposes of Article III standing. *See, e.g., In re Anthem,*
22 *Inc. Data Breach Litig.* (“*Anthem I*”), 162 F. Supp. 3d 953, 985 (N.D. Cal. 2016) (finding
23 plaintiffs alleged benefit of the bargain losses where plaintiffs alleged that they did not receive full
24 value of services for which they paid because of defendant’s failure to implement promised
25 security measures); *In re LinkedIn User Privacy Litig.*, 2014 WL 1323713, at *6 (N.D. Cal. Mar.
26 28, 2014) (finding plaintiff alleged lost benefit of the bargain, and thus standing under Article III,
27 where plaintiff alleged that she purchased defendant’s services because defendant represented the

1 services as secure, that defendant’s services were not in fact secure, and thus plaintiff overpaid for
2 defendant’s services as a result of defendant’s misrepresentations). Again, Defendants do not
3 address Neff’s benefit of the bargain losses in their motion to dismiss, and Defendants do not
4 argue that these losses are insufficient to allege an injury-in-fact. *See* Mot. at 21–22. For these
5 reasons, Neff’s allegations of benefit of the bargain losses are sufficient to allege an Article III
6 injury in fact.

7 **d. Summary**

8 To summarize, the Court finds that all Plaintiffs have adequately alleged an injury in fact
9 sufficient for Article III standing because all Plaintiffs have alleged a risk of future identity theft,
10 in addition to loss of value of their PII. Moreover, some Plaintiffs, although not all Plaintiffs, have
11 adequately alleged additional injuries in fact in the form of (1) harm from the actual misuse of
12 their PII; (2) out-of-pocket mitigation expenses; and (3) lost benefit of the bargain. The Court
13 next turns to Defendants’ traceability argument.

14 **2. Traceability**

15 Defendants next contend that, even assuming Plaintiffs have adequately alleged injuries in
16 fact, Plaintiffs cannot establish Article III standing because Plaintiffs’ injuries are not “fairly
17 traceable” to Defendants’ conduct. *See* Mot. at 22. Defendants make two primary arguments.
18 First, Defendants contend that there is no “causal connection between the information stolen” from
19 Defendants and the injuries claimed by Plaintiffs. Second, Defendants contend that “other causes”
20 exist for Plaintiffs’ alleged harms. The Court considers each of these arguments in turn.

21 **a. Causal Connection between Information Stolen and Plaintiffs’ Alleged
22 Harms**

23 First, Defendants argue that the sensitive personal information allegedly taken from
24 Plaintiffs by hackers—such as Plaintiffs’ Social Security Numbers—was not itself collected by
25 Defendants. *See* Mot. at 23–24. Defendants contend that, “[t]o the extent Social Security
26 numbers or any other specific personal information were communicated via Yahoo email at all,”
27 that information was contained in and accessed by hackers from Plaintiffs’ emails inside of

1 Plaintiffs' Yahoo email accounts. *Id.* Thus, Defendants argue, Plaintiffs' alleged harm is the
2 result of "the pre-breach activities of Plaintiffs," rather than Defendants themselves. *Id.*

3 Defendants' argument is not persuasive. First of all, Yahoo itself possessed sensitive
4 personal information, such as credit card numbers, for small business users such as Neff, who paid
5 Yahoo \$13.95 every month. As to other plaintiffs, "for Article III standing purposes, a 'causal
6 chain does not fail simply because it has several links, provided those links are not hypothetical or
7 tenuous and remain plausible.'" *Moore v. Apple, Inc.*, 309 F.R.D. 532, 540 (N.D. Cal. 2015)
8 (quoting *Wsh. Env'tl Council v. Bellon*, 732 F. 3d 1131, 1141–42 (9th Cir. 2013)). Here, as
9 discussed above, Plaintiffs allege that they were all Yahoo account holders. Plaintiffs allege that,
10 during the Data Breaches, hackers obtained the names, email addresses, recovery email accounts,
11 telephone numbers, birth dates, passwords, security questions and answers, and account "nonce"
12 (a cryptographic value unique to each account) of Yahoo account holders. CCAC ¶¶ 1, 92. As a
13 result of gaining this information, the hackers were able to gain "access to the email contents of all
14 breached Yahoo accounts and thus any private information contained within those emails." *Id.*
15 Plaintiffs detail in the CCAC the numerous ways that Plaintiffs used their Yahoo emails for their
16 personal communications and finances, and thus Plaintiffs allege that their Yahoo email accounts
17 contained sensitive personal information, such as Plaintiffs' credit and debit card account
18 information and Plaintiffs' Social Security numbers. *See, e.g., id.* ¶¶ 10–15, 42–44.

19 Plaintiffs thus allege a plausible "causal chain" of events that links the Data Breaches,
20 which Plaintiffs allege resulted from Yahoo's failures to maintain appropriate data security
21 measures, with the specific harms alleged by Plaintiffs. Indeed, Plaintiffs' allegations are
22 substantially similar to the allegations in *Anthem*, in which this Court held that the plaintiffs had
23 alleged a sufficiently plausible "logical connection between the Anthem data breach and the harm
24 suffered by Plaintiffs." *Anthem I*, 162 F. Supp. 3d at 987. In *Anthem*, the plaintiffs alleged that
25 (1) "they were enrolled in a particular health plan administered by" Anthem, that (2) plaintiffs
26 "provided their PII to Anthem," (3) "that their PII was compromised as a result of the data
27 breach," and (4) that their PII was used by hackers for "illicit financial gain." *Id.* Plaintiffs have

1 alleged substantially the same chain of events here. *See, e.g.*, CCAC ¶¶ 1, 10–15.

2 Defendants attempt to distinguish *Anthem* by arguing that the *Anthem* plaintiffs, unlike
3 Plaintiffs here, provided their Social Security numbers and other sensitive personal information
4 *directly* to Anthem. *See* Reply at 8. Accordingly, Defendants argue that the *Anthem* plaintiffs’
5 sensitive personal information was *directly* disclosed to hackers when the hackers breached
6 Anthem’s servers. *Id.* In the instant Data Breaches, by contrast, Defendants argue that Plaintiffs’
7 Social Security numbers and other sensitive PII was not *directly* collected by Defendants, and thus
8 Plaintiffs’ sensitive PII was not *directly* exposed to hackers during the breaches of Defendants’
9 servers. *Id.* Rather, hackers stole from Defendants the names, email addresses, recovery email
10 accounts, telephone numbers, birth dates, passwords, security questions and answers, and account
11 nonce of Yahoo account holders, CCAC ¶¶ 1, 92, and *then* the hackers used that information to
12 gain access to Plaintiffs’ Yahoo emails where the hackers found Plaintiffs’ Social Security
13 numbers and other sensitive personal information. *See* Reply at 8.

14 However, this distinction does not defeat traceability for purposes of Article III standing.
15 Although Plaintiffs in the instant case allege an additional link in the “causal chain”—specifically,
16 that the hackers first stole Plaintiffs’ log-in information from Yahoo and *then* accessed the
17 sensitive personal information contained within Plaintiffs’ email accounts—the links alleged by
18 Plaintiffs nonetheless “remain plausible.” *Moore*, 309 F.R.D. at 540 (“[A] ‘causal chain does not
19 fail simply because it has several links, provided those links are not hypothetical or tenuous and
20 remain plausible.’”). Plaintiffs set forth numerous allegations in the CCAC that plausibly explain
21 how Plaintiffs and other Yahoo users used their Yahoo email accounts for their personal and
22 financial needs. *See, e.g.*, CCAC ¶¶ 1, 10–15, 43–44. Plaintiffs allege that their email accounts
23 contained Plaintiffs’ sensitive personal and financial information, including their Social Security
24 numbers and/or their credit and debit card account information. *Id.* ¶¶ 10–15. Plaintiffs allege
25 that, as a result of Defendants’ lax data security practices and the Data Breaches, hackers were
26 able to *continually* access Plaintiffs’ Yahoo email accounts and the sensitive information
27 contained within Plaintiffs’ Yahoo email accounts. *Id.* ¶ 68. Taking these allegations as true,

1 Plaintiffs have sufficiently alleged a plausible chain of events that link Defendants’ alleged
2 misconduct with the injuries alleged by Plaintiffs.

3 The causal chain alleged in this case is distinguishable from the causal chain alleged in
4 *Antman v. Uber Technologies, Inc.*, 2015 WL 6123054, at *10–11 (N.D. Cal. Oct. 19, 2015), the
5 case relied upon by Defendants. There, hackers breached Uber’s servers and gained access to the
6 names and drivers’ license information of Uber drivers. *Id.* at *2. The Court in *Antman* held that
7 the plaintiff failed to allege a sufficiently plausible causal connection between the breach of
8 Uber’s servers and the plaintiff’s allegations of identity theft. *Id.* at *11. As the Court reasoned in
9 *Antman*, the plaintiff alleged “disclosure only of his name and driver’s license information,” and it
10 was not plausible that a hacker could open a credit card in the plaintiff’s name only from this
11 information. *Id.* The plaintiff in *Antman* alleged no further facts to suggest a connection between
12 the information stolen—his name and driver’s license information—and his allegations that the
13 hackers stole his identity and opened a credit card in his name. *Id.*

14 In contrast to the plaintiff in *Antman*, Plaintiffs in the instant case have alleged that (1)
15 Defendants’ data security practices were insufficient; (2) hackers accordingly breached
16 Defendants’ servers and learned of Plaintiffs’ names, email addresses, recovery email accounts,
17 telephone numbers, birth dates, passwords, security questions and answers, and account nonce,
18 CCAC ¶¶ 1, 92; and (3) hackers accordingly gained access to Plaintiffs’ Yahoo email accounts,
19 which contained additional PII, including PII such as Social Security numbers and debit and credit
20 card account information. *See* CCAC ¶¶ 1, 10–15, 44. Plaintiffs allege that, as a result of this
21 causal chain, Plaintiffs suffer from an increased risk of identity theft, loss of the value of their PII,
22 harms from actual identity theft, out-of-pocket mitigation expenses, and lost benefit of the bargain,
23 as detailed in the injury-in-fact discussion above. At this stage of the litigation, Plaintiffs’
24 allegations are sufficient to show that Plaintiffs’ alleged injuries are “fairly traceable” to
25 Defendants’ alleged misconduct.

26 **b. “Other Causes” for Plaintiffs’ Alleged Harms**

27 Next, Defendants argue that Plaintiffs have failed to allege traceability because “other

1 causes exist” for the harms alleged by Plaintiffs, such as other data breaches. *See* Mot. at 25–26.
 2 Defendants argue that these “other causes” are potentially likely here, given that Plaintiffs allege
 3 that their information was exposed as early as 2013, but Plaintiffs allege identity theft and
 4 unauthorized credit card charges beginning in 2016 and later. *See id.*

5 Again, the Court is not persuaded by Defendants’ arguments. To the extent Defendants
 6 rely on the existence of other data breaches to defeat a causal connection between the Data
 7 Breaches here and Plaintiffs’ injuries, this Court squarely rejected an identical argument in *Anthem*
 8 *I*, 162 F. Supp. 3d at 988. As the Court explained in *Anthem I*, to allow Defendants to rely on
 9 other data breaches to defeat a causal connection would “create a perverse incentive for
 10 companies: so long as enough data breaches take place, individual companies will never be found
 11 liable.” *Id.* As set forth above, Plaintiffs have plausibly alleged that Plaintiffs had accounts with
 12 Yahoo, that Plaintiffs’ account information was accessed in the Data Breaches, and that hackers
 13 used Plaintiffs’ account information to gain access to Plaintiffs’ Yahoo email accounts, which
 14 contained additional sensitive PII. The existence of other potential data breaches or causes for
 15 Plaintiffs’ injuries does not defeat Plaintiffs’ standing to sue Defendants. *Anthem I*, 162 F. Supp.
 16 3d at 988 (rejecting defendants’ argument that “scores of other cyber intrusions and data thefts”
 17 could have caused plaintiffs alleged injuries).³

18 Moreover, Defendants’ reliance on temporal gaps in time between the Data Breaches and
 19 Plaintiffs’ allegations of identity theft and unauthorized charges also does not defeat traceability in
 20 this case. For example, Plaintiff alleges that “[i]n August 2016, a hacker identifying himself or
 21

22 ³ Defendants also argue that “[n]o Plaintiff has alleged that his or her email address (as well as
 23 certain other data elements) was not publicly available,” and thus accessible regardless of the Data
 24 Breaches. *See* Mot. at 26. However, Defendants’ argument is “little more than an end run around
 25 the rule that, on a motion to dismiss, the Court may generally ‘consider only the contents of the
 26 complaint,’” and the Court must take the complaint’s allegations as true and in the light most
 27 favorable to Plaintiffs. *In re Anthem, Inc. Data Breach Litigation*, 162 F. Supp. 3d at 988.
 Plaintiffs do not allege that their Yahoo email addresses, recovery email accounts, telephone
 28 numbers, birth dates, passwords, security questions and answers, and account nonce, CCAC ¶¶ 1,
 92, were publicly available elsewhere, *see* CCAC ¶ 1, and the Court cannot infer otherwise on a
 motion to dismiss. *See Manzarek*, 519 F.3d at 1031 (holding that on a motion to dismiss, the court
 “accept[s] factual allegations in the complaint as true and construe[s] the pleadings in the light
 most favorable to the nonmoving party.”).

1 herself as ‘peace_of_mind’ posted for sale on the dark web the PII from 200 million Yahoo
2 accounts.” CCAC ¶ 70. As recently as March 17, 2017, stolen information from the Data
3 Breaches “was still for sale on underground hacker forums.” *Id.* ¶ 84. Specifically, the CCAC
4 contains screenshots of hackers selling documents labeled as “Yahoo, 100K, email: pass,
5 decrypted,” and “Yahoo, 5,737,977, decrypted, complete.” *Id.* Plaintiffs allege that “identity
6 thieves will wait years before attempting to use the PII they have obtained.” *Id.* ¶ 40.
7 Accordingly, even though the Data Breaches themselves occurred as early as 2013, Plaintiffs have
8 sufficiently alleged that the harms Plaintiffs are experiencing today are a direct result of the Data
9 Breaches. Thus, the temporal gap between the Data Breaches and Plaintiffs’ alleged harm does
10 not defeat traceability.

11 To summarize, the Court concludes that Plaintiffs have sufficiently demonstrated both a
12 logical and a temporal relationship necessary to establish traceability between Defendants’ alleged
13 misconduct and Plaintiffs’ alleged injuries. Accordingly, because the Court found above that
14 Plaintiffs have all adequately alleged an injury in fact, the Court finds that Plaintiffs have
15 sufficiently alleged Article III standing to sue. Thus, Defendants’ motion to dismiss on the basis
16 of Plaintiffs’ lack of Article III standing is DENIED. The Court next turns to address Plaintiffs’
17 causes of action.

18 **B. UCL**

19 The United States Plaintiffs and Israel Plaintiffs allege in Count One a claim under the
20 California UCL against Yahoo. Small Business Users Plaintiff Neff alleges in Count Eleven a
21 claim under the UCL against both Yahoo and Aabaco, the wholly owned subsidiary of Yahoo that
22 administered Yahoo’s small business services. However, although alleged as separate counts, the
23 allegations under Count One and Count Eleven are substantially the same. Accordingly, the Court
24 considers Plaintiffs’ UCL claims together below and specifies distinctions between the two UCL
25 claims only when necessary.

26 California’s UCL provides a cause of action for business practices that are (1) unlawful;
27 (2) unfair; or (3) fraudulent. Cal. Bus. & Prof. Code § 17200, et seq. “The UCL’s coverage is

1 sweeping, and its standard for wrongful business conduct intentionally broad.” *Moore v. Apple,*
 2 *Inc.*, 73 F. Supp. 3d 1191, 1204 (N.D. Cal. 2014) (internal quotation marks omitted). Each prong
 3 of the UCL provides a “separate and distinct theory of liability.” *Lozano v. AT&T Wireless Servs.,*
 4 *Inc.*, 504 F.3d 718, 731 (9th Cir. 2007). Although the UCL targets a wide range of misconduct, its
 5 remedies are limited because UCL actions are equitable in nature.” *Pom Wonderful LLC v. Welch*
 6 *Foods, Inc.*, 2009 WL 5184422, at *2 (C.D. Cal. Dec. 21, 2009). “Remedies for private
 7 individuals bringing suit under the UCL are limited to restitution and injunctive relief.” *Id.*

8 Plaintiffs bring their UCL claims under all three prongs of the UCL. Defendants argue,
 9 however, that Plaintiffs’ UCL claims fail for several reasons. First, Defendants argue that
 10 Plaintiffs lack standing to bring claims under the UCL. Second, Defendants argue that Plaintiffs
 11 have failed to plead that Defendants’ actions were either unlawful, unfair, or fraudulent. Third,
 12 Defendants argue that Plaintiffs are not entitled to the remedies that they seek under the UCL, and
 13 thus their UCL claims must be dismissed. The Court addresses each of these three arguments
 14 below.

15 1. UCL Standing

16 In order to establish standing for a UCL claim, Plaintiffs must show that they personally
 17 lost money or property “as a result of the unfair competition.” Cal. Bus. & Prof. Code § 17204;
 18 *Kwikset Corp. v. Sup. Ct.*, 51 Cal. 4th 310, 330 (2011). As the California Supreme Court has
 19 explained:

20 There are innumerable ways in which economic injury from unfair
 21 competition may be shown. A plaintiff may (1) surrender in a
 22 transaction more, or acquire in a transaction less, than he or she
 23 otherwise would have; (2) have a present or future property interest
 24 diminished; (3) be deprived of money or property to which he or she
 25 has a cognizable claim; (4) be required to enter into a transaction,
 26 costing money or property, that would otherwise have been
 27 unnecessary.

28 *Id.* at 323.

According to Plaintiffs, all named Plaintiffs have experienced injury under the UCL.
 Specifically, Plaintiffs argue that Small Business Users Plaintiff Neff has adequately alleged lost

1 money or property because Neff has “benefit of the bargain” losses as a result of Neff’s payments
 2 to Defendants for Defendants’ Small Business Services. Moreover, Plaintiffs argue that the
 3 United States Plaintiffs and Israel Plaintiffs, who did not pay Defendants to use Defendants’ email
 4 services,⁴ have nonetheless alleged lost money or property because (1) five out of the six United
 5 States Plaintiffs have alleged out-of-pocket expenses resulting from the Data Breaches; and (2) *all*
 6 Plaintiffs have alleged a risk of future identity theft.

7 The Court first discusses Neff’s allegations of lost benefit of the bargain. The Court then
 8 discusses Plaintiffs’ allegations regarding the United States Plaintiffs and the Israel Plaintiffs, and
 9 whether these Plaintiffs can allege lost money or property as a result of their out of pocket
 10 expenses or the risk of future identity theft.

11 **a. Lost Benefit of the Bargain**

12 Plaintiffs argue that Small Business Users Plaintiff Neff has adequately alleged standing
 13 under the UCL because Neff has alleged lost benefit of the bargain. The Court agrees.

14 Neff alleges that he has paid Defendants \$13.94 each month since September 2009 for
 15 Defendants’ Small Business Services. CCAC ¶ 20. Neff alleges that Defendants represented that
 16 Defendants’ Small Business Services were “secure.” *Id.* ¶ 198. Neff alleges that he “would not
 17 have agreed to utilize and pay for the small business services and turn over [his] PII” had Neff
 18 known that Defendants’ Small Business Services “were not as secure as represented or secure by
 19 any standard.” *See, e.g., id.* at ¶ 199. Accordingly, Neff alleges that he was “damaged by paying
 20 monthly fees to [Defendants] for something [Neff] did not receive: secure small business
 21 services.” *Id.* ¶ 203.

22 As set forth above regarding Neff’s Article III standing to sue, these allegations are
 23

24 ⁴ Israel Plaintiff Rivlin alleges in passing that he pays Yahoo annually \$20.00 “to have Yahoo
 25 emails received forwarded to another email account.” CCAC ¶ 15. However, Plaintiffs do not
 26 argue that Rivlin has suffered lost benefit of the bargain as a result of his \$20.00 annual payment
 27 to Yahoo, and indeed Plaintiffs do not otherwise address Rivlin’s \$20.00 annual payment in their
 28 opposition or in the CCAC. *See generally* Opp.; CCAC. Accordingly, the Court considers only
 whether Neff has adequately alleged lost benefit of the bargain, and the Court does not address
 whether Rivlin can adequately allege lost benefit of the bargain based on his \$20.00 annual
 payment to Yahoo.

1 sufficient to allege that Neff suffered “benefit of the bargain” losses. *See, e.g., Anthem II*, 2016
2 WL 3029783, at *15, 30 (finding allegations that plaintiffs spent more money on insurance
3 premiums than plaintiffs would have spent had plaintiffs known of Anthem’s inadequate security
4 practices to be sufficient to allege benefit of the bargain losses). Benefit of the bargain losses are
5 sufficient to allege “lost money or property,” and thus standing, under the UCL. *See id.* (finding
6 plaintiffs’ alleged benefit of the bargain losses were sufficient to establish standing under the
7 UCL); *see also In re Adobe*, 66 F. Supp. 3d at 1224 (finding allegations that plaintiffs “personally
8 spent more on Adobe products than they would have had they known Adobe was not providing
9 the reasonable security Adobe represented it was providing” to be sufficient to allege standing
10 under the UCL). Accordingly, the Court finds that Small Business Users Plaintiff Neff has
11 adequately alleged standing under the UCL, and the Court DENIES Defendants’ motion to
12 dismiss Neff’s UCL claim for lack of UCL standing.

13 **b. Out of Pocket Expenses and Risk of Future Harm**

14 The Court next turns to whether the United States Plaintiffs and the Israel Plaintiffs have
15 adequately alleged UCL standing. Unlike Small Business Users Plaintiff Neff, the United States
16 Plaintiffs and the Israel Plaintiffs did not pay for their Yahoo email accounts, and accordingly
17 these Plaintiffs cannot allege benefit of the bargain losses. However, Plaintiffs argue that the
18 United States Plaintiffs and Israel Plaintiffs nonetheless can allege “lost money or property” as a
19 result of Defendants’ conduct. Specifically, five of the United States Plaintiffs allege that they
20 incurred out-of-pocket expenses as a result of the Data Breaches. Moreover, Plaintiffs argue that
21 *all* Plaintiffs have alleged a risk of future identity theft. For the reasons discussed below, the
22 Court agrees with Plaintiffs that, to the extent Plaintiffs allege out-of-pocket expenses as a result
23 of the Data Breaches, Plaintiffs have alleged lost money or property sufficient to establish UCL
24 standing. However, the Court disagrees with Plaintiffs’ argument that the risk of future identity
25 theft is sufficient for UCL standing purposes.

26 First, Plaintiffs argue that United States Plaintiffs Heines, Essar, Dugas, Matthew Ridolfo,
27 and Deana Ridolfo allege that they incurred out-of-pocket expenses as a result of the Data

1 Breaches. For example, Plaintiffs Essar, Matthew Ridolfo, and Deana Ridolfo all allege that, as a
 2 result of the Data Breaches and their identities being stolen as a result of the Data Breaches, they
 3 have paid money for credit monitoring services. *See, e.g.*, CCAC ¶¶ 11, 13. Moreover, Heines
 4 alleges that she was required to pay late fees because she was unable to pay her bills on time after
 5 her Social Security Disability benefits were taken from her Social Security Disability account. *Id.*
 6 ¶ 10. Dugas alleges that, as a result of his identity being stolen in the Data Breaches and a false
 7 tax return being filed in his name, Dugas paid credit bureaus to freeze his accounts, and he had to
 8 pay a Certified Public Accountant to “help sort out the tax return problems suffered as a result of
 9 the” Data Breaches. *Id.*

10 The Court finds that these allegations plausibly suggest that Plaintiffs Heines, Essar,
 11 Dugas, Matthew Ridolfo, and Deana Ridolfo were each “required to enter into a transaction,
 12 costing money or property, that would otherwise have been unnecessary” if not for Defendants’
 13 alleged misconduct. *Kwikset*, 246 P.3d at 885–86; *see also Anthem I*, 162 F. Supp. 3d at 986–87
 14 (suggesting, without needing to decide, that out of pocket expenses resulting from a data breach
 15 would fall under *Kwikset*’s definition of economic injury). Indeed, courts have held similar
 16 allegations of out of pocket expenses sufficient to establish standing under the UCL. *See, e.g.*,
 17 *Witriol v. LexisNexis Grp.*, 2006 WL 4725713, at *6 (N.D. Cal. Feb. 10, 2006) (finding plaintiffs
 18 adequately alleged economic injury under the UCL where plaintiffs alleged that they had
 19 “incurred costs associated with monitoring and repairing credit” after a data breach (internal
 20 quotation marks omitted)); *Walters, LLC*, 2017 WL 1398660, at *2 (finding plaintiff alleged
 21 economic injury sufficient to establish standing under the UCL where the plaintiff alleged that he
 22 was required to monitor his credit after the theft of his payment card data in a data breach).
 23 Accordingly, the Court DENIES Defendants’ motion to dismiss for lack of UCL standing the UCL
 24 claims of Plaintiffs Heines, Essar, Dugas, Matthew Ridolfo, and Deana Ridolfo.

25 The Court next turns to the remaining United States Plaintiffs and Israel Plaintiffs, who do
 26 not allege any benefit of the bargain losses or out of pocket expenses resulting from the Data
 27 Breach. Specifically, United States Plaintiff Garg, and both Israel Plaintiffs Rivlin and Granot, do

1 not allege that they lost any money or property as a result of Defendants’ alleged misconduct.⁵
 2 Nonetheless, Plaintiffs argue that Plaintiffs Garg, Rivlin, and Granot have standing under the UCL
 3 because *all* Plaintiffs face an “imminent risk of future costs” resulting from the Data Breaches.
 4 *See Opp.* at 21. Plaintiffs argue that this is sufficient under the UCL to allege “lost money or
 5 property,” and thus UCL standing. *Id.*

6 The Court disagrees with Plaintiffs. Plaintiffs’ imminent risk of *future* costs as a result of
 7 the Data Breaches, although sufficient to establish standing under the broader injury-in-fact
 8 requirements of Article III, is not sufficient to allege “lost money or property” under the UCL.
 9 *See Ehret v. Uber Tech., Inc.*, 68 F. Supp. 3d 1121, 1132 (N.D. Cal. Sept. 17, 2014) (“[A] federal
 10 plaintiff’s [Article III] ‘injury in fact’ may be intangible and need not involve lost money or
 11 property . . . a UCL plaintiff’s ‘injury in fact’ [must] specifically involve lost money or
 12 property.”). Plaintiffs’ “intangible” allegations of future costs do not show that Plaintiffs have
 13 “specifically . . . lost money or property” as a result of Defendants’ misconduct. *Id.* Accordingly,
 14 the Court finds that Plaintiffs Garg, Rivlin, and Granot, have not sufficiently alleged standing
 15 under the UCL. Thus, the Court GRANTS Defendants’ motion to dismiss the UCL claims of
 16 Garg, Rivlin, and Granot. The Court grants leave to amend because Plaintiffs Garg, Rivlin, and
 17 Granot may be able to allege facts sufficient to show that they have lost money or property as a
 18 result of Defendants’ conduct, and thus amendment of these claims would not necessarily be
 19 futile. *See Leadsinger*, 512 F.3d at 532 (holding that leave to amend is proper when amendment is
 20 not futile).

21 The Court next turns to whether Plaintiffs have adequately alleged that Defendants violated
 22 the UCL, either under the unlawful, unfair, or fraudulent prongs. Significantly, because the Court
 23

24 ⁵ As set forth above, Israel Plaintiff Rivlin alleges in passing that he pays Yahoo annually \$20.00
 25 “to have Yahoo emails received forwarded to another email account.” CCAC ¶ 15. However,
 26 Plaintiffs do not address Rivlin’s \$20.00 annual payment in their opposition or in the CCAC, and
 27 Plaintiffs do not argue that this \$20.00 constitutes a lost out of pocket expense or lost benefit of
 28 the bargain. *See generally Opp.*; CCAC. Accordingly, based on the allegations in the CCAC,
 Rivlin’s \$20.00 annual payment for forwarding services does not establish that Rivlin has lost
 money or property as a result of Defendants’ unlawful conduct, and thus does not establish that
 Rivlin has standing under the UCL.

1 has found that Plaintiffs Rivlin and Granot—the only Israel Plaintiffs—have not adequately
 2 alleged UCL standing, the Court’s remaining UCL discussion below will consider the allegations
 3 of only the United States Plaintiffs and Small Business Users Plaintiff Neff. Because the Court
 4 has dismissed the UCL claims of the only two Israel Plaintiffs, the Israel Class cannot state a UCL
 5 claim. As stated above, the dismissal of the UCL claims of the Israel Plaintiffs, and thus the Israel
 6 Class, is without prejudice because amendment of these claims would not necessarily be futile.

7 **2. Defendants’ Liability Under Unlawful, Unfair, and Fraudulent Prongs**

8 As set forth above, the UCL provides a cause of action for business practices that are (1)
 9 unlawful, (2) unfair, or (3) fraudulent. Cal. Bus. & Prof. Code § 17200. Each prong of the UCL
 10 provides a separate and distinct theory of liability. *Lozano*, 504 F.3d at 731. Plaintiffs allege that
 11 Defendants’ conduct violated all three prongs of the UCL. *See* CCAC ¶¶ 127, 214. The Court
 12 addresses these three prongs below in turn.

13 **a. Unlawful Prong**

14 First, Plaintiffs argue that Defendants violated the unlawful prong. The “unlawful” prong
 15 of the UCL prohibits “anything that can properly be called a business practice and that at the same
 16 time is forbidden by law.” *Cal-Tech*, 20 Cal. 4th at 180 (internal quotation marks omitted). By
 17 proscribing “any unlawful” business practice, the UCL permits injured consumers to “borrow”
 18 violations of other laws and treat them as unlawful competition that is independently actionable.
 19 *Id.*

20 As predicates for their claim under the “unlawful” prong, Plaintiffs allege that Defendants
 21 violated the California Legal Remedies Act, Cal. Civ. Code § 1750 (“CLRA”); the Customer
 22 Records Act, Cal. Civ. Code § 1798.80 (“CRA”); the Stored Communications Act, 18 U.S.C.
 23 § 2702 (“SCA”); and the Online Privacy Protection Act, Cal. Bus. & Prof. Code §§ 22576
 24 (“OPPA”). *See* CCAC ¶ 134.

25 In addition to asserting violations of these statutes as predicates for the unlawful prong of
 26 Plaintiffs’ UCL claims, the CCAC also asserts stand-alone causes of action for each of these
 27 statutes. CCAC ¶¶ 137–76 (Causes of Action 2–5). To the extent that Plaintiffs have sufficiently
 28

1 alleged these stand-alone causes of action, Plaintiffs have also alleged violations of the unlawful
 2 prong of the UCL. The Court addresses Plaintiffs' allegations under these statutes in detail below.
 3 *See infra* Part III.D–G. As explained below, the Court finds that Plaintiffs have adequately
 4 alleged that Defendants violated the CRA. “Accordingly, the Court finds that Plaintiffs have
 5 adequately alleged unlawful conduct that may serve as a basis for a claim under the UCL’s
 6 unlawful prong, and [Defendants are] therefore not entitled to dismissal of the UCL unlawful
 7 claim.” *In re Adobe*, 66 F. Supp. 3d at 1226 (finding Plaintiffs adequately alleged UCL claim
 8 under unlawful prong where plaintiff adequately alleged underlying CRA violation). Thus, the
 9 Court DENIES Defendants’ motion to dismiss Plaintiffs’ UCL claim under the unlawful prong.

10 **b. Unfair Prong**

11 The “unfair” prong of the UCL creates a cause of action for a business practice that is
 12 unfair even if not proscribed by some other law. *Korea Supply Co. v. Lockheed Martin Corp.*, 29
 13 Cal. 4th 1134, 1143 (2003). “The UCL does not define the term ‘unfair’ . . . [and] the proper
 14 definition of ‘unfair’ conduct against consumers ‘is currently in flux’ among California courts.”
 15 *Id.*

16 Some California courts apply a balancing approach, which requires courts to “weigh the
 17 utility of the defendant’s conduct against the gravity of the harm to the alleged victim.” *Davis v.*
 18 *HSBC Bank Nevada, N.A.*, 691 F.3d 1152, 1169 (9th Cir. 2012) (internal quotation marks
 19 omitted). Other California courts have held that “unfairness must be tethered to some legislatively
 20 declared policy or proof of some actual or threatened impact on competition.” *Lozano*, 504 F.3d
 21 at 735 (internal quotation marks omitted). Finally, one California court has adopted the three-part
 22 test set forth in § 5 of the Federal Trade Commission Act: “(1) the consumer injury must be
 23 substantial; (2) the injury must not be outweighed by any countervailing benefits to consumers or
 24 competition; and (3) it must be an injury that consumers themselves could not reasonably have
 25 avoided.” *Camacho v. Auto. Club of Southern Cal.*, 48 Cal. Rptr. 3d 770, 777 (Cal. Ct. App.
 26 2006). The Court refers to these tests as the “balancing test,” the “tethering test,” and the “FTC
 27 test,” respectively.

1 The Court finds that Plaintiffs’ allegations are sufficient at this stage of the proceedings to
2 allege that Defendants’ conduct violated the balancing test, at a minimum. Plaintiffs “may
3 proceed with a UCL claim under the balancing test by either alleging immoral, unethical,
4 oppressive, unscrupulous or substantially injurious conduct by Defendants *or* by demonstrating
5 that Defendants’ conduct violated an established public policy.” *Anthem I*, 162 F. Supp. 3d at 990.
6 Here, Plaintiffs allege that Defendants promised in their Privacy Policy to protect their customers’
7 data, but that Defendants knowingly failed to employ adequate safeguards to protect their
8 customers’ data, in violation of Defendants’ Privacy Policy. *See, e.g.*, CCAC ¶¶ 128–33.
9 Moreover, Plaintiffs allege that Defendants’ knowing failure to employ adequate safeguards
10 violated the policy of various California statutes, such as the Online Privacy Protection Act, that
11 were intended to “reflect California’s public policy of protecting customer data.” *Anthem I*, 162 F.
12 Supp. 3d at 990. Plaintiffs allege that Defendants’ misconduct exposed Plaintiffs to a substantial
13 risk of identity theft and other harms. *See, e.g.*, CCAC ¶ 135.

14 District courts have found substantially identical allegations sufficient to allege “unfair”
15 conduct under the balancing test. *See, e.g., Anthem I*, 162 F. Supp. 3d at 990 (finding plaintiffs
16 adequately alleged unfair conduct under the balancing test where the complaint alleged that
17 defendant failed to adequately protect customer data, which was allegedly in violation of several
18 statutes that reflected California’s public policy of protecting customer data); *In re Adobe*, 66 F.
19 Supp. 3d at 1227 (finding plaintiffs adequately alleged unfair conduct under the balancing test
20 where plaintiffs alleged Adobe’s conduct violated various data breach statutes that embodied
21 California’s public policy of protecting customer data); *Svenson v. Google, Inc.*, 2015 WL
22 1503429, at *10 (N.D. Cal. Apr. 1, 2015) (finding plaintiffs sufficiently alleged violation of
23 UCL’s unfair prong where plaintiffs alleged that “Google violated its own privacy policies” by
24 failing to safeguard the plaintiff’s data). As this Court recognized in *Anthem I*, whether
25 Defendants’ alleged “public policy violation is outweighed by the utility of their conduct under the
26 balancing test is a question to be resolved at a later stage in this litigation.” *Anthem I*, 162 F.
27 Supp. 3d at 990 (N.D. Cal. 2016). Thus, based on the balancing test alone, the Court DENIES

1 Defendants' motion to dismiss Plaintiffs' UCL claim under the unfair prong.

2 **c. Fraudulent Prong**

3 "To state a claim under the 'fraud' prong of [the UCL], a plaintiff must allege facts
4 showing that members of the public are likely to be deceived by the alleged fraudulent business
5 practice." *Antman*, 2015 WL 6123054, at *6. Claims stated under the fraud prong of the UCL are
6 subject to the particularity requirements of Federal Rule of Civil Procedure 9(b). *Kearns v. Ford*
7 *Motor Co.*, 567 F.3d 1120, 1125 (9th Cir. 2009). Under Rule 9(b), "[i]n alleging fraud or
8 mistake, a party must state with particularity the circumstances constituting fraud or mistake."
9 Fed. R. Civ. P. 9(b). Plaintiffs must include "an account of the time, place, and specific content of
10 the false representations" at issue. *Swartz v. KPMG LLP*, 476 F.3d 756 (9th Cir. 2007).

11 Plaintiffs allege two theories of fraud under the UCL: (1) affirmative misrepresentations;
12 and (2) fraudulent omissions. The Court considers each in turn.

13 **i. Affirmative Misrepresentations**

14 Plaintiffs allege that Defendants committed fraud through affirmative misrepresentations.
15 Specifically, Plaintiffs allege that Defendants made affirmative misrepresentations to the United
16 States Plaintiffs and Small Business Users Plaintiff Neff in Defendants' Privacy Policy.
17 Moreover, Plaintiffs allege that Defendants made additional affirmative misrepresentations to
18 Small Business Users Plaintiff Neff in Defendants' advertisements regarding Defendants' Small
19 Business Services. The Court first addresses the representations in Defendants' Privacy Policy
20 and then discusses Defendants' Small Business Services.

21 **1. Privacy Policy**

22 Plaintiffs allege Defendants made the following representations in Defendants' Privacy
23 Policy:

- 24 • "[P]rotecting our systems and our users' information is paramount to ensuring Yahoo users
25 enjoy a secure user experience and maintaining our users' trust."
- 26 • Defendants had "physical, electronic, and procedural safeguards that comply with federal
27 regulations to protect personal information about you."

1 CCAC ¶ 128. Plaintiffs allege that these representations in Defendants’ Privacy Policy were false
2 because Defendants “knew or should have known [they] did not employ reasonable measures that
3 would have kept Plaintiffs’ and the other Class members’ PII and financial information secure and
4 prevented the loss of Plaintiffs’ and the other class members’ PII and financial information.” *Id.* ¶
5 130. Defendants argue, however, that Plaintiffs have failed to state a UCL claim based on
6 Defendants’ representations in its Privacy Policy because (1) Defendants’ statements are not
7 actionable misrepresentations; and (2) Plaintiffs have failed to adequately allege that they relied on
8 the representations in Defendants’ Privacy Policy. *See Mot.* at 28–29. The Court considers these
9 arguments in turn.

10 First, Defendants contend that Plaintiffs cannot state a claim under the fraudulent prong
11 because a reasonable consumer would not rely on the representations. Claims under “California
12 consumer protection statutes are governed by the ‘reasonable consumer’ test.” *Ebner v. Fresh,*
13 *Inc.*, 838 F.3d 958, 965 (9th Cir. 2016). “Under this standard, Plaintiff must ‘show that members
14 of the public are likely to be deceived.’” *Id.* (internal quotation marks and citations omitted).
15 “[W]hether a business practice is deceptive will usually be a question of fact not appropriate for
16 decision on demurrer.” *Williams v. Gerber Prods. Co.*, 552 F.3d 934, 938 (9th Cir. 2008).
17 However, Plaintiff must allege “more than a mere possibility that the [statement] might
18 conceivably be misunderstood by a few consumers viewing it in an unreasonable manner.” *Brod*
19 *v. Sious Honey Ass’n, Co-Op*, 927 F. Supp. 2d 811, 828 (N.D. Cal. 2013) (citing *Lavie v. Proctor*
20 *& Gamble Co.*, 105 Cal. App. 4th 496, 508 (Cal. 2003)). Rather, the reasonable consumer
21 standard requires a probability “that a significant portion of the general consuming public or of
22 targeted consumers, acting reasonably in the circumstances, could be misled.” *Lavie*, 105 Cal.
23 App. 4th at 508.

24 According to Defendants, a reasonable consumer could not have been deceived by the
25 alleged misrepresentations because they are “non-actionable puffery.” *See Mot.* at 28.
26 “[G]eneralized, vague, and unspecified assertions[] constitute[] ‘mere puffery’ upon which a
27 reasonable consumer could not rely,” and thus are not actionable under the UCL. *Glen Holly*

1 *Entm't, Inc. v. Tektronix Inc.*, 343 F.3d 1000, 1005 (9th Cir. 2003). As the Ninth Circuit has
 2 explained, “[t]he common theme that seems to run through cases considering puffery in a variety
 3 of contexts is that consumer reliance will be induced by specific rather than general assertions.”
 4 *Cook, Perkiss and Liehe, Inc. v. No. Cal. Collection Serv., Inc.*, 911 F.2d 242, 246 (9th Cir. 1990)
 5 (“‘Puffing’ has been described by most courts as involving outrageous generalized statements, not
 6 making specific claims, that are so exaggerated as to preclude reliance by consumers.”); *see also*
 7 *Newcal Indus., Inc. v. Ikon Office Solution*, 513 F.3d 1038, 1053 (9th Cir. 2008) (“A statement is
 8 considered puffery if the claim is extremely unlikely to induce consumer reliance. Ultimately, the
 9 difference between a statement of fact and mere puffery rests in the specificity or generality of the
 10 claim.”). Consequently, a representation “which merely states in general terms that one product is
 11 superior is not actionable. However, misdescriptions of specific or absolute characteristics of a
 12 product are actionable.” *Cook*, 911 F.2d at 246 (citations and internal quotation marks omitted).

13 As set forth above, the CCAC alleges that Defendants made two misrepresentations in its
 14 Privacy Policy: (1) that “protecting our systems and our users’ information is paramount to
 15 ensuring Yahoo users enjoy a secure user experience and maintaining our users’ trust”; and (2)
 16 that Defendants had “physical, electronic, and procedural safeguards that comply with federal
 17 regulations to protect personal information about you.”

18 The Court agrees with Defendants that the first alleged misrepresentation—that “protecting
 19 our systems and our users’ information is paramount to ensuring Yahoo users enjoy a secure user
 20 experience and maintaining our users’ trust”—constitutes non-actionable puffery. This statement
 21 “say[s] nothing about the specific characteristics” of the products and services offered by
 22 Defendants. *Elias v. Hewlett-Packard Co.*, 903 F. Supp. 2d 843, 855 (N.D. Cal. Oct. 11, 2012).
 23 Rather, the statement is a vague and “all-but-meaningless superlative[.]” regarding how
 24 Defendants’ prioritize the safety of their systems and their users’ information. *Id.* (quoting
 25 *Consumer Advocates v. Echostar Satellite Corp.*, 113 Cal. App. 4th 1351, 1361)). A reasonable
 26 consumer could not rely on this statement as describing the security of Defendants’ servers. *See,*
 27 *e.g., Lloyd v. CVB Fin. Corp.*, 811 F.3d 1200, 1206–07 (9th Cir. 2016) (finding company’s

1 statement that “strong credit culture and underwriting integrity remain paramount at CVB” to be
2 non-actionable puffery). Thus, to the extent Plaintiffs base their fraudulent misrepresentation
3 claim on Defendants’ statement that “protecting our systems and our users’ information is
4 paramount to ensuring Yahoo users enjoy a secure user experience and maintaining our users’
5 trust,” the Court GRANTS Defendants’ motion to dismiss. The Court grants with prejudice
6 because, as a matter of law, the Court finds that this statement is mere puffery on which a
7 reasonable consumer could not rely. *See Baltazar v. Apple Inc.*, 2011 WL 6747884, at *4 (N.D.
8 Cal. Dec. 22, 2014) (“If an alleged misrepresentation would not deceive a reasonable consumer or
9 amounts to mere puffery, then the claim may be dismissed as a matter of law.”).

10 However, the Court finds that the second alleged misrepresentation—that Defendants had
11 “physical, electronic, and procedural safeguards that comply with federal regulations to protect
12 personal information about you”—is not puffery. Unlike the statement discussed above, this
13 second alleged misrepresentation makes a “specific, non-subjective guarantee” that Defendants
14 use safeguards that complied with federal regulations to protect users’ information. *Andersen v.*
15 *Griswold Int’l, LLC*, 2014 WL 12694138, at *6 (N.D. Cal. Dec. 16, 2014). A reasonable
16 consumer could rely on this statement as representing that Defendants did, in fact, use safeguards
17 that complied with federal regulations. More generally, a reasonable consumer could rely on this
18 statement as representing that Defendants’ safeguards, which were represented to comply with
19 federal regulations, were sufficient to protect users’ information from ordinary data security
20 threats. Plaintiffs allege that Defendants’ privacy safeguards did *not* comply with applicable laws
21 and regulations relating to data security, and that Defendants’ privacy safeguards were *not*
22 sufficient to protect users’ information from ordinary data security threats. To the contrary,
23 Plaintiffs allege that Yahoo’s “data encryption protocol” was “widely discredited and had been
24 proven, many years prior, easy to break.” *See, e.g.*, CCAC ¶ 133. Thus, in the context of the
25 instant allegations, Defendants’ representation that it used safeguards that complied with federal
26 regulations to protect users’ information is not puffery.

27 Defendants further contend in their motion that Defendants’ statement that Defendants

1 have “physical, electronic, and procedural safeguards that comply with federal regulations to
 2 protect personal information about you” is non-actionable because Defendants represented
 3 elsewhere in the Privacy Policy that Defendants’ systems were not “100% secure,” and that their
 4 systems have “inherent limitations.” *See* Mot. at 29–30. The Court disagrees. A reasonable
 5 consumer could rely on Defendants’ representations that Defendants had “physical, electronic, and
 6 procedural safeguards that comply with federal regulations to protect information about you,” but
 7 still understand that no computer system is “100% secure” and that all computer systems have
 8 “inherent limitations.” The crux of Plaintiffs’ allegations is not that Defendants safeguards failed
 9 to be “100% secure.” Rather, the crux of Plaintiffs’ allegations is that Defendants’ safeguards did
 10 not comply with applicable laws and regulations and that Defendants’ data encryption protocol
 11 was “widely discredited and had been proven, many years prior, easy to break.” *See* CCAC ¶ 133.
 12 In the context of Plaintiffs’ allegations, Defendants’ statement that Defendants had safeguards that
 13 complied “with federal regulations to protect information about you” is actionable as fraud, even
 14 though Defendants also represented that their systems were not “100% secure” and that they had
 15 “inherent limitations.”

16 Second, Defendants contend that, even assuming Plaintiffs have alleged an actionable
 17 misrepresentation, Plaintiffs’ UCL fraud claim fails because Plaintiffs have failed to adequately
 18 allege reliance. “California courts have held that when the ‘unfair competition’ underlying a
 19 plaintiff’s UCL claim consists of a defendant’s misrepresentation or omission,” a plaintiff must
 20 plead that he or she “actually relied on the misrepresentation or omission” to bring a UCL claim.
 21 *Backhaut v. Apple, Inc.*, 74 F. Supp. 3d 1033, 1047 (N.D. Cal. 2014) (citing *In re Tobacco II*
 22 *Cases*, 46 Cal. 4th 298, 326 (2009)). “This showing of actual reliance under the UCL requires a
 23 plaintiff to allege that ‘the defendant’s misrepresentation or nondisclosure was an immediate cause
 24 of the plaintiff’s injury-producing conduct.” *Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1190,
 25 1220 (N.D. Cal. 2014) (quoting *In re Tobacco II*, 46 Cal. 4th at 326). “A plaintiff may establish
 26 that the defendant’s misrepresentation is an immediate cause of the plaintiff’s conduct by showing
 27 that in its absence the plaintiff in all reasonable probability would not have engaged in the injury-

1 producing conduct.” *Id.* (internal quotation marks omitted). “While a plaintiff need not
 2 demonstrate that the defendant’s misrepresentations were ‘the sole or even the predominant or
 3 decisive factor influencing his conduct,’ the misrepresentations must have ‘played a substantial
 4 part’ in the plaintiff’s decision making.” *Id.*

5 As set forth above, the alleged misrepresentation that Defendants had “physical, electronic,
 6 and procedural safeguards that comply with federal regulations to protect personal information
 7 about you” is contained within Defendants’ Privacy Policy. Defendants’ Privacy Policy is
 8 incorporated via hyperlink into Defendants’ Terms of Service. *See* CCAC, Ex. 2. Plaintiffs
 9 contend all users “were required to view and accept [Defendants’ Terms of Service] prior to
 10 creating their accounts and providing their PII” to Defendants. *See, e.g.* CCAC ¶ 128. According
 11 to Plaintiffs, they have adequately alleged reliance on Defendants’ Privacy Policy because they
 12 had to accept Defendants’ Terms of Service to create their accounts. Defendants contend,
 13 however, that Plaintiffs have not adequately alleged actual reliance for purposes of their fraudulent
 14 prong claim because Plaintiffs do not allege that they *actually read* the Privacy Policy.

15 The Court agrees with Defendants. “[T]his Court has consistently held that plaintiffs in
 16 misrepresentation cases must allege that they actually read the challenged representations” in order
 17 to state a claim. *Perkins*, 53 F. Supp. 3d at 1220; *see also, e.g., In re iPhone Application Litig.*, 6
 18 F. Supp. 3d 1004, 1018 (N.D. Cal. 2013) (“[N]one of the Plaintiffs presents evidence that he or she
 19 even saw, let alone read and relied upon, the alleged misrepresentations contained in the Apple
 20 Privacy Policies”). As this Court explained in *Perkins*, “the fact that [] the alleged
 21 misrepresentations appeared on screens that all users had to click through to register” for the
 22 defendant’s website does not “establish that any of the Plaintiffs actually read or relied on the
 23 misrepresentations in the absence of allegations that Plaintiffs read these statements.” *Perkins*, 53
 24 F. Supp. 3d at 1220.

25 Here, although all Plaintiffs had to click through Defendants’ Terms of Service in order to
 26 create their accounts, *see* CCAC ¶ 116, Plaintiffs do not allege that they “actually read”
 27 Defendants’ Terms of Service, let alone that Plaintiffs “actually read” the separate Privacy Policy

1 containing the alleged misrepresentation at issue, which was accessible within Defendants’ Terms
 2 of Service via an *additional* hyperlink. *Id.* Thus, as the Court held in *Perkins*, Plaintiffs have not
 3 adequately alleged a UCL fraud claim based on misrepresentations in Defendants’ Privacy Policy
 4 because Plaintiffs have not adequately alleged that they “actually relied” on Defendants’
 5 misrepresentation contained within Defendants’ Privacy Policy. *Id.*; *see also, e.g., In re LinkedIn*
 6 *User Privacy Litig.*, 932 F. Supp. 2d 1089, 1093 (N.D. Cal. 2013) (“Plaintiffs do not even allege
 7 that they actually read the alleged misrepresentation—the Privacy Policy—which would be
 8 necessary to support a claim of misrepresentation.”).

9 Accordingly, the Court GRANTS Defendants’ motion to dismiss Plaintiffs’ UCL fraud
 10 claim to the extent that it is based on Defendants’ affirmative misrepresentation that Defendants
 11 had “physical, electronic, and procedural safeguards that comply with federal regulations to
 12 protect personal information about you.” The Court grants Plaintiffs leave to amend this claim
 13 because Plaintiffs may be able to allege that Plaintiffs actually relied upon this alleged
 14 misrepresentation, and thus leave to amend is not necessarily futile. *See Leadsinger*, 512 F.3d at
 15 532 (holding that leave to amend is proper when amendment is not futile).

16 **2. Small Business Services Advertisements**

17 In addition to the alleged misrepresentations contained within Defendants’ Privacy Policy,
 18 Small Business Users Plaintiff Neff further alleges that Defendants made representations to users
 19 of Defendants’ Small Business Services in Defendants’ advertisements for their Small Business
 20 Services. *See* CCAC ¶¶ 98–99. Plaintiffs allege that Neff and all customers of Defendants’ Small
 21 Business Services “were exposed to and read these advertisements and explanations, which appear
 22 on the webpages all customers must use to sign-up for the services.” *Id.* ¶ 97.

23 Plaintiffs excerpt several representations in Defendants’ Small Business Services
 24 advertisements, including:

- 25 • “It’s easy to create a professional-looking website. Reassure customers with the VeriSign
 26 Verified Seal”
- 27 • “Password protection is available for your accounts and sections of your website
 28 (Advanced and Premier plans only)”

- 1 • “Your website runs on a Unix operating system and Apache servers”
- 2 • “Shared SSL certificates and encryption protect the information customers submit to your
- 3 site (Advanced and Premier plans only)”

4 See CCAC ¶¶ 98–99. For several reasons, the Court finds that Plaintiffs have not adequately
5 alleged a UCL fraud claim premised on these statements in Defendants’ Small Business Services
6 advertisements.

7 First, Defendants’ statement that “[i]t’s easy to create a professional-looking website” is a
8 generalized and “highly subjective” statement, and thus constitutes mere puffery that is not
9 actionable as a matter of law. See *Southland Sod Farms v. Stover Seed Co.*, 108 F.3d 1134, 1145
10 (9th Cir. 1997) (noting that “highly subjective” statements that constitute “generalized boasting”
11 are puffery “upon which no reasonable buyer would rely”).

12 Second, in order to plead fraud with particularity under Rule 9(b), Plaintiffs “must explain
13 why the statement or omission complained of was false and misleading.” *Mazur v. eBay Inc.*,
14 2008 WL 618988, at *13 (N.D. Cal. Mar. 4, 2008). Significantly, Plaintiffs’ CCAC includes only
15 screenshots of the above representations in Defendants’ Small Business Services advertisements,
16 but Plaintiffs do not explain why any of these statements are false and misleading. See CCAC ¶¶
17 98–99. For example, Plaintiffs do not allege that Defendants’ representations that “[s]hared SSL
18 certificates and encryption protect the information customers submit to your site,” that customers
19 of small business websites can be “[r]eassure[d]” with a “VeriSign Verified Seal,” and that small
20 business websites “run[] on Unix operating system and Apache servers” are, indeed, false. See *id.*
21 Absent any allegations in the CCAC explaining “what makes the representations false” or
22 misleading, Plaintiffs have not adequately stated a fraud claim premised on these
23 misrepresentations under Rule 9(b). *Gallegos v. Wells Fargo Bank, N.A.*, 2013 WL 3166389, at
24 *3 (E.D. Cal. June 20, 2013) (explaining that, to meet the heightened pleading standard of Rule
25 9(b), a plaintiff must “explain what makes the misrepresentations false”). Indeed, although
26 Plaintiffs excerpt these advertisements in the CCAC’s general factual allegations, Plaintiffs do not
27 refer to Defendants’ Small Business Services advertisements at all in Plaintiffs’ UCL claims. See,

1 e.g., CCAC ¶¶ 213–22.

2 Accordingly, the Court GRANTS Defendants’ motion to dismiss Plaintiffs’ UCL fraud
3 claim to the extent it is premised on Defendants’ alleged misrepresentations in its Small Business
4 Services advertisements. The Court grants Plaintiffs leave to amend their claim because Plaintiffs
5 maybe able to allege with particularity why Defendants’ representations are false.⁶ See
6 *Leadsinger*, 512 F.3d at 532 (holding that leave to amend is proper when amendment is not futile).

7 **ii. Fraudulent Omissions**

8 Plaintiffs also allege that Defendants violated the UCL’s fraudulent prong through
9 fraudulent omissions. For an omission to be actionable under the UCL, “the omission must be
10 contrary to a representation actually made by the defendant, or an omission of a fact the defendant
11 was obliged to disclose.” *Daugherty v. Am. Honda Motor Co.*, 144 Cal. App. 4th 824, 835 (2006).
12 The California Courts of Appeal have held that there are four circumstances in which a duty to
13 disclose may arise: “(1) when the defendant is the plaintiff’s fiduciary; (2) when the defendant has
14 exclusive knowledge of a material fact not known or reasonably accessible to the plaintiff; (3)
15 when the defendant actively conceals a material fact from the plaintiff; [or] (4) when the defendant
16 makes partial representations that are misleading because some other material fact has not been
17 disclosed.” *Collins v. eMachines, Inc.*, 202 Cal. App. 4th 249, 255 (2011). “[A] fact is deemed
18 ‘material,’ and obligates an exclusively knowledgeable defendant to disclose it, if a ‘reasonable
19

20 ⁶ Small Business Users Plaintiff Neff also alleges in Count Nine and Count Ten a claim against
21 Defendants for fraudulent inducement and negligent misrepresentation, respectively. Neff alleges
22 in these counts that Defendants “made numerous representations, in advertising and in the Privacy
23 Policy, regarding the supposed secure nature of their small business services,” and that Neff
24 “reasonably relied on the[se] representations.” See, e.g. ¶¶ 198–99. Neff does not identity any
25 specific misrepresentations. Thus, as set forth above, the Court concludes that Neff either cannot
26 allege an actionable misrepresentation, or cannot allege reliance on an actionable
27 misrepresentation. This holding defeats Neff’s claims for fraudulent inducement and negligent
28 misrepresentation, which also require an actionable misrepresentation and actual reliance. See,
e.g., Hinesley v. Oakshade Town Ctr., 135 Cal. App. 4th 289, 367, 371 (Cal. Ct. App. 2005)
(setting forth elements for fraudulent inducement, including a “misrepresentation” and “actual
reliance”); *B.L.M. v. Sabo & Deitsch*, 55 Cal. App. 4th 823, 834–38 (Cal. Ct. App. 1997) (setting
forth elements for negligent misrepresentation, including “misrepresentation” and “actual
reliance”). Thus, for the reasons set forth above with regards to Neff’s UCL claim for fraud, the
Court GRANTS with leave to amend Defendants’ motion to dismiss Neff’s claims for fraudulent
inducement and negligent misrepresentation.

1 [consumer]’ would deem it important in determining how to act in the transaction at issue.” *Id.* at
 2 256 (citing *Engalla v. Permanente Med. Grp., Inc.*, 15 Cal. App. 4th 951, 977 (1997)).

3 Plaintiffs contend that Defendants were required to disclose the fact of Defendants’ “non-
 4 compliant and substandard security systems.” *See, e.g.*, CCAC ¶ 103. Defendants contend,
 5 however, that even assuming Defendants had a duty to disclose to Plaintiffs that Defendants’
 6 security systems were “non-compliant” and “substandard,” Plaintiffs nonetheless cannot state a
 7 UCL claim because Plaintiffs fail to plead actual reliance on the omission of that information. For
 8 the reasons discussed below, the Court agrees with Defendants.

9 As discussed above, “California courts have held that when the ‘unfair competition’
 10 underlying a plaintiff’s UCL claim consists of a defendant’s misrepresentation or omission,” a
 11 plaintiff must plead that he or she “actually relied on the misrepresentation or omission” to bring a
 12 UCL claim. *Backhaut*, 74 F. Supp. 3d at 1047 (citing *In re Tobacco II Cases*, 46 Cal. 4th at 326).
 13 Actual reliance on the omission of material information can be shown where the plaintiff alleges
 14 that, “had the omitted information been disclosed, [the plaintiff] *would have been aware of it* and
 15 behaved differently.” *Ehrlich v. BMW of N.A., Inc.*, 801 F. Supp. 2d 908, 919 (C.D. Cal. 2010)
 16 (quoting *Mirkin*, 5 Cal. 4th at 1093).

17 As discussed above, Plaintiffs do not allege that they actually read Defendants’ Privacy
 18 Policy. Accordingly, to the extent Plaintiffs’ UCL fraudulent omission claim is based on
 19 Defendants’ failure in their Privacy Policy to disclose that their security systems were non-
 20 compliant and substandard, Plaintiffs have not alleged that, had Defendants disclosed in their
 21 Privacy Policy that Defendants’ security systems were non-compliant and substandard, Plaintiffs
 22 “*would have been aware*” of this disclosure. *See id.* (finding that plaintiff failed to plead actual
 23 reliance on omitted information where plaintiff failed to allege that “he reviewed any brochure,
 24 website, or promotional material that might have contained a disclosure of the cracking defect”).
 25 Accordingly, the Court GRANTS Defendants’ motion to dismiss Plaintiffs’ UCL fraud claim to
 26 the extent that it is based on Defendants’ allegedly fraudulent omissions in their Privacy Policy.
 27 The Court grants Plaintiffs leave to amend because Plaintiffs may be able to allege that Plaintiffs

1 would have been aware of the allegedly omitted information had Defendants disclosed that
2 information in their Privacy Policy. *See Leadsinger*, 512 F.3d at 532 (holding that leave to amend
3 is proper when amendment is not futile).

4 However, Small Business User Plaintiff Neff alleges that all customers of Defendants’
5 Small Business Services, “including Plaintiff Neff, were exposed to and read [the Small Business
6 Services] advertisements and explanations, which appear on the webpages all customers must use
7 to sign-up for the services.” CCAC ¶ 97. Neff alleges that Defendants’ online security “was
8 highly material to [his] decision to utilize Defendants’ Small Business services,” but that
9 Defendants did not disclose to Neff that their online security was non-compliant and substandard.
10 *See id.* Accordingly, Neff has alleged that, had Defendants disclosed in their Small Business
11 Services advertisements that their security systems were non-compliant and substandard, Neff
12 “would have been aware” of these disclosures, and Neff would have “behaved differently.”
13 *Ehrlich*, 801 F. Supp. 2d at 919 (quoting *Mirkin*, 5 Cal. 4th at 1093). Thus, to the extent
14 Plaintiffs’ UCL fraud claim is based on Defendants’ allegedly fraudulent omissions to Small
15 Business Plaintiff Neff and the putative Small Business Users Class in Defendants’ Small
16 Business Services advertisements, the Court DENIES Defendants’ motion to dismiss.

17 **3. Entitlement to UCL Remedies**

18 Lastly, Defendants argue that Plaintiffs’ UCL claim must be dismissed because Plaintiffs
19 have not sufficiently alleged entitlement to equitable relief, which is the only relief available under
20 the UCL. *See Mot.* at 30; *see Pom Wonderful*, 2009 WL 5184422, at *2 (“Although the UCL
21 targets a wide range of misconduct, its remedies are limited because UCL actions are equitable in
22 nature.”).

23 However, as Defendants appear to concede, Neff has standing to seek restitution on behalf
24 of the putative Small Business Users Class. *See Reply* at 11–12 (arguing only that Plaintiffs have
25 failed to establish entitlement to seek injunctive relief). “Under the UCL, an individual may
26 recover profits unfairly obtained to the extent that these profits represent monies given to the
27 defendant or benefits in which the plaintiff has an ownership interest.” *Id.* Here, Neff alleges that

1 Defendants represented that their servers were secure and that Neff paid Defendants for
2 Defendants' Small Business Services, but that Defendants knowingly failed to undertake
3 reasonable security measures to protect Neff's personal information. As a result, Neff alleges that
4 Neff lost the benefit of the bargain, and that Defendants unfairly obtained profits from Neff.
5 These allegations are sufficient to demonstrate that Neff may seek restitution. *See, e.g., Anthem I,*
6 *162 F. Supp. 3d at 986* (finding plaintiffs adequately alleged entitlement to restitution where
7 plaintiffs adequately alleged lost benefit of the bargain as a result of defendant's lax data security
8 measures).

9 Plaintiffs concede that the United States Plaintiffs, who did not pay for Defendants'
10 services, cannot seek restitution from Defendants. *See Opp.* at 26. Because United States
11 Plaintiffs did not pay for Defendants' services, the United States Plaintiffs did not give Defendants
12 money "or benefits in which [Plaintiffs] have an ownership interest." *See Pom Wonderful LLC,*
13 *2009 WL 5184422, at *2.* Nonetheless, Plaintiffs argue that the United States Plaintiffs have
14 standing to seek injunctive relief against Defendants. *See Opp.* at 26. The Court agrees. To
15 establish standing for prospective injunctive relief, a plaintiff must demonstrate that he or she "has
16 suffered or is threatened with a concrete and particularized legal harm, coupled with a sufficient
17 likelihood that he [or she] will again be wronged in a similar way." *Bates v. United Parcel Serv.,*
18 *Inc., 511 F.3d 974, 985 (9th Cir. 2007).* "As to the second inquiry, [a plaintiff] must establish a
19 'real and immediate threat of repeated injury.'" *Id.* (quoting *O'Shea v. Littleton, 414 U.S. 488,*
20 *496 (1974)*). "[P]ast wrongs do not in themselves amount to [a] real and immediate threat of
21 injury necessary to make out a case or controversy." *City of Los Angeles v. Lyons, 416 U.S. 95,*
22 *111 (1983).*

23 Defendants argue that Plaintiffs have alleged only a "past wrong" resulting from the Data
24 Breaches, and Plaintiffs do not face a "real and immediate threat of" future injury. *Lyons, 416*
25 *U.S. at 111.* However, a fair reading of the CCAC is that, although Defendants "claim[] to have
26 plugged the leaks" in their security systems, Plaintiffs cannot trust Defendants' representations
27 regarding their security systems. Accordingly, Plaintiffs face a "real and immediate threat" of

1 further disclosure of their PII, which remains in the hands of Defendants. *See Lyons*, 416 U.S. at
 2 111; *see, e.g.*, CCAC ¶¶ 84–85. Moreover, Plaintiffs allege that at least “as late as March 17,
 3 2017,” hackers have been actively selling the PII of Defendants’ users on the dark web. CCAC ¶
 4 84. Plaintiffs allege that Defendants have not only failed to take any actions with regard to this
 5 information being on the dark web, but that Defendants have continued to dispute the scope of
 6 their responsibility. *See id.* ¶¶ 84–96. Taking these allegations as true and in the light most
 7 favorable to Plaintiffs, the Court finds that Plaintiffs have adequately alleged a “real and
 8 immediate threat of repeated injury” from Defendants. *See Bates*, 511 F.3d at 985. Accordingly,
 9 at this stage of the litigation, Plaintiffs have adequately alleged standing to seek injunctive relief
 10 under the UCL. Thus, the Court DENIES Defendants’ motion to dismiss Plaintiffs’ UCL claim
 11 for lack of entitlement to UCL remedies.

12 C. CLRA

13 In Count Two, the United States Plaintiffs and the Israel Plaintiffs assert a claim against
 14 Yahoo under the CLRA, which prohibits “unfair methods of competition and unfair or deceptive
 15 acts or practices undertaken by any person in a transaction intended to result or which results in
 16 the sale or lease of goods or services to any consumer.” Cal. Civ. Code § 1770(a).

17 Defendants move to dismiss Plaintiffs’ CLRA claim on three grounds. First, Defendants
 18 argue that “Yahoo accounts are free, so Plaintiffs are not ‘consumers’ under the CLRA.” *See Mot.*
 19 at 30. Second, Defendants argue that Yahoo’s email platform does not qualify as a “good” or
 20 “service” within the meaning of the CLRA. *Id.* Third, Defendants argue that Plaintiffs do not
 21 sufficiently allege reliance as required for a CLRA claim. *Id.* As discussed further below, the
 22 Court finds that dismissal is appropriate because Plaintiffs are not consumers under the CLRA,
 23 and thus the Court need not consider Defendants’ remaining arguments.

24 As stated above, the CLRA prohibits certain unfair methods of competition “in the sale or
 25 lease of goods or services to any consumer.” Cal. Civ. Code § 1770(a). The CLRA defines a
 26 “consumer” as “an individual who seeks or acquires, by purchase or lease, any goods or services
 27 for personal, family, or household purposes.” Cal. Civ. Code § 1761(d). Thus, in order to state a
 28

1 claim under the CLRA, Plaintiffs must sufficiently allege, among other things, that they are
2 “consumers” because they “purchase[d] or lease[d]” some good or service of Defendants. *Id.*

3 Significantly, only the United States Plaintiffs and Israel Plaintiffs assert a CLRA claim.⁷
4 However, these Plaintiffs used Yahoo’s free email service and thus did not “purchase or lease” a
5 good or service from Defendants.⁸ *See* Cal. Civ. Code § 1761(d). In their opposition, Plaintiffs
6 insist that they can nonetheless state a CLRA claim because Defendants “collect and store
7 tremendous amounts of PII, and use this information to maximize profits through targeted
8 advertising and other means.” *See* Opp. at 17–18. Accordingly, Plaintiffs argue that “use of their
9 Yahoo accounts is *not* ‘free.’” *Id.* Moreover, Plaintiffs argue that their allegations are sufficient
10 given the CLRA’s “liberal mandate.” *Id.*

11 Contrary to Plaintiffs’ argument, the fact that Defendants store PII and use this PII for
12 targeted advertising does not indicate that Plaintiffs “purchase[d] or lease[d]” some good or
13 service within the meaning of the CLRA. *See* Cal. Civ. Code § 1761(d). Indeed, district courts in
14 this Circuit have rejected substantially identical arguments. In *Claridge v. RockYou, Inc.*, 785 F.
15 Supp. 2d 855 (N.D. Cal. 2011), the plaintiff asserted a CLRA claim based on a data breach of
16 RockYou, “a publisher and developer of online services and applications for use with social
17 networking sites.” *Id.* at 858. RockYou moved to dismiss the CLRA claim on the ground that

18
19 _____
20 ⁷ Small Business Users Plaintiff Neff does not assert a CLRA claim on behalf of the putative
21 Small Business Users Class. This is likely because, as discussed above, the CLRA applies only to
22 those who purchased or leased goods or services “for personal, family, or household purposes,”
23 and does not include purchasers of goods or services for business purposes. Cal. Civ. Code §
24 1761(d).

25 ⁸ The Court notes that the CCAC alleges in passing that Plaintiff Rivlin, one of the Israel
26 Plaintiffs, “pays Yahoo annually \$20.00 to have Yahoo emails received forwarded to another
27 email account.” *See* CCAC ¶ 15. However, this is the only mention in the CCAC of this email
28 forwarding service, and Plaintiffs do not mention this email forwarding service in Plaintiffs’
opposition as a ground for their CLRA claim. To the extent Plaintiffs seek to state a CLRA claim
based on Rivlin’s use of this paid email forwarding service, the CCAC does not allege any “unfair
methods of competition and unfair or deceptive acts or practices . . . intended to result or which
results in the sale or lease” of this email forwarding service. *See* Cal. Civ. Code § 1770(a). Nor
does the CCAC allege that this email forwarding service was for “personal, family, or household
purposes,” as required to state a CLRA claim. *Id.* § 1761(d). Accordingly, to the extent Plaintiffs
seek to state a CLRA claim based on Rivlin’s use of a paid email forwarding service, Plaintiffs
have not adequately alleged such a claim.

1 plaintiff was not a consumer because the plaintiff’s RockYou account was free and thus the
2 plaintiff did not “purchase or lease” a good or service from RockYou. *Id.* at 864. In response, the
3 plaintiff argued that “because his PII has an ascertainable value and constitutes both currency and
4 property, his transfer of PII information to defendant in exchange for free applications, constitutes
5 a purchase or lease under the CLRA.” *Id.* (internal quotation marks omitted). However, the
6 *Claridge* court rejected this argument, and found that the “notion that the phrase ‘purchase’ or
7 ‘lease’ contemplates any less than tangible form of payment . . . finds no support under the
8 specific statutory language of the CLRA, nor has plaintiff relied on any legal authority suggesting
9 as much.” *Id.* at 864.

10 Another court in this district, following *Claridge*, has also rejected a plaintiff’s argument
11 “that he purchased the defendant’s services with his PII” for the purposes of the CLRA. *See*
12 *Yunker v. Pandora Media, Inc.*, 2013 WL 1282980, at *12 (N.D. Cal. Mar. 26, 2013); *see also*
13 *Song Fi, Inc. v. Google, Inc.*, 2016 WL 1298999, at *12 (N.D. Cal. Apr. 4, 2016) (“Providing
14 consumer traffic for YouTube, Plaintiffs’ alleged consideration, is certainly a less than tangible
15 form of payment.”). Additionally, the Third Circuit has followed *Claridge* and *Yunker* and come
16 to a similar conclusion. *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d
17 125, 153 (3d Cir. 2015), *cert. denied*, 137 S. Ct. 36 (2016) (rejecting plaintiffs argument that for
18 the purposes of the CLRA, the plaintiffs engaged in a “‘sale’ whereby they gave their trackable
19 internet history information in exchange for advertisements delivered to their browsers (i.e., the
20 ‘services’”).

21 The Court finds the reasoning of these cases persuasive. The mere fact that Yahoo gained
22 some profit from Plaintiffs’ use of Yahoo’s free email services does not by itself show that
23 Plaintiffs “purchased” those services from Defendants. *See Claridge*, 785 F. Supp. at 864
24 (rejecting the “notion that the phrase ‘purchase’ or ‘lease’ contemplates any less than tangible
25 form of payment” under the CLRA). Additionally, as in *Claridge*, Plaintiffs cite no legal
26 authority—and the Court is not aware of any legal authority—to support Plaintiffs’ theory that the
27 mere transfer of PII renders Plaintiffs’ use of a free service a “purchase” or “lease” of that service.

1 *See id.* Furthermore, as the Court recognized in *Claridge*, Plaintiffs’ references to the “CLRA’s
 2 liberal mandate,” *see* Opp. at 28, do not allow the Court to ignore the clear text of the CLRA,
 3 which requires a “purchase or lease.” *See Claridge*, 785 F. Supp. 2d at 864 (noting that the
 4 “purchase or lease” of goods or services is “a strict requirement under the statute”). The Court
 5 cannot ignore the CLRA’s “strict requirement” of a “purchase or lease” simply because Plaintiffs
 6 believe that the result is unfair in this case. *See id.*

7 Accordingly, the Court finds that United States Plaintiffs and Israel Plaintiffs have not
 8 alleged any “purchase or lease” and therefore cannot assert a CLRA claim. Thus, the Court
 9 GRANTS Defendants’ motion to dismiss Plaintiffs’ CLRA claim. The Court cannot find at this
 10 stage that amendment would necessarily be futile. Therefore, the Court grants leave to amend.
 11 *See Leadsinger*, 512 F.3d at 532 (holding that leave to amend is proper when amendment is not
 12 futile).

13 **D. Customer Records Act**

14 The United States Plaintiffs, Israel Plaintiffs, and Small Business Users Plaintiff assert a
 15 claim in Count Three under the California Customer Records Act (“CRA”), Cal. Civ. Code §
 16 1798.80, *et seq.* The CRA “regulates businesses with regard to treatment and notification
 17 procedures relating to their customers’ personal information.” *Corona v. Sony Pictures Ent’mt*,
 18 2015 WL 3916744, at *6 (C.D. Cal. June 15, 2015). Plaintiffs allege that Defendants violated §
 19 1798.82 of the CRA. This provision provides, in relevant part:

20 A person or business that conducts business in California, and that
 21 owns or licenses computerized data that includes personal
 22 information, shall disclose a breach of the security of the system
 23 following discovery or notification of the breach in the security of
 the data to a resident of California (1) whose unencrypted personal
 information was, or is reasonably believed to have been, acquired by
 an unauthorized person

24 Cal. Civ. Code § 1798.82(a). The statute requires that disclosure “shall be made in the most
 25 expedient time possible and without unreasonable delay.” *Id.* The statute also describes the
 26 information that must be included in the security breach notification and the form that the security
 27 breach notification must take. *See* § 1798.82(d).

United States District Court
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

Section 1798.82(h) defines “personal information” for purposes of the CRA as the following:

(1) An individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

- (A) Social security number.
- (B) Driver’s license number or California identification number.
- (C) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.
- (D) Medical information.
- (E) Health insurance information
- (F) Information or data collected through the use or operation of an automated license plate recognition system . .

(2) A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

See Cal. Civ. Code § 1798.82(h).

Plaintiffs contend that the Data Breaches at issue constituted “breach[es] of the security” of Defendants’ systems, that Plaintiffs’ “personal information was,” or was reasonable believed by Defendants to have been, “acquired by an unauthorized person” during the Data Breaches, and that Defendants unreasonably delayed informing Plaintiffs about the Data Breaches, in violation of § 1798.82. *See* Cal. Civ. Code § 1798.82; CCAC ¶¶ 151–52.

Defendants move to dismiss Plaintiffs’ CRA claim on several bases. First, Defendants argue that the non-California Plaintiffs lack standing to bring a CRA claim. Second, Defendants argue that they were not required to notify Plaintiffs about the 2013 Breach. Third, Defendants argue that they were not required to notify Plaintiffs about the Forged Cookie Breach. Finally, Defendants argue that Plaintiffs have failed to allege damages resulting from Defendants’ violation of the CRA. The Court considers each of these arguments in turn.

1. Standing for Non-California Residents

First, Defendants move to dismiss the CRA claims of non-California residents because, according to Defendants, non-California residents lack standing to bring claims under the CRA.

1 The Court agrees with Defendants. As set forth above, the plain language of the CRA provides
 2 that a California business that owns computerized data that includes personal information “shall
 3 disclose a breach of the security of the system following discovery or notification of the breach in
 4 the security of the data *to a resident of California*” whose information was acquired by an
 5 unauthorized person. Cal. Civ. Code § 1798.82(a) (emphasis added). Given this language, district
 6 courts have dismissed CRA claims brought on behalf of non-California Plaintiffs because the
 7 CRA “is clear that it applies only ‘to ensure the personal information [of] California residents is
 8 protected.’” *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 942,
 9 973 (S.D. Cal. Oct. 11, 2012) (quoting Cal. Civ. Code § 1798.81.5(a)); *see also Antman*, 2015 WL
 10 6123054, at *5 (“Section 1798.82 has procedures for notifying *California residents* when their
 11 unencrypted personal information is disclosed in a data breach and thereby acquired (or
 12 reasonably believed to have been acquired by) an unauthorized person” (citing Cal. Civ. Code §
 13 1798.82(a)(emphasis added)).

14 Plaintiffs make two primary arguments in opposition to Defendants, neither of which is
 15 persuasive. First, Plaintiffs argue that § 1798.84(b), which is the remedies provision of the CRA,
 16 provides that “[a]ny customer injured by a violation of this title may institute a civil action to
 17 recover damages.” *See* Opp. at 31 (quoting Cal. Civ. Code § 1798.84(b)). Plaintiffs read the
 18 language “*any customer*” to mean that the CRA is not geographically limited. *Id.* (emphasis
 19 added). However, § 1798.84(b) provides a private right of action to “[a]ny customer *injured by a*
 20 *violation*” of the CRA. Cal. Civ. Code § 1798.84(b) (emphasis added). As set forth above, a
 21 business violates the CRA if the business fails to notify “*a resident of California*” that the
 22 resident’s personal information was acquired or reasonably believed to have been acquired by an
 23 unauthorized person. *See* Cal. Civ. Code § 1798.82(a) (emphasis added). Accordingly, a non-
 24 California resident cannot as a matter of law be “injured by a violation” of the CRA, Cal. Civ.
 25 Code § 1798.84(b), because under the plain language of § 1798.82(a), a non-California resident
 26 has no right to receive notification of a data breach. *See* Cal. Civ. Code § 1798.82(a). Thus,
 27 Plaintiffs’ reliance on the remedies provision of the CRA is unavailing.

1 Second, Plaintiffs argue that non-California Plaintiffs can bring claims under the CRA
2 because Defendants have stipulated “to the nationwide application of California law.” *See* Opp. at
3 31–32. However, as the Ninth Circuit has held, “[w]hen a law contains geographical limitations
4 as to its application, courts will not apply it to parties falling outside those limitations even if the
5 parties stipulate that the law should apply.” *Fred Briggs Distributing Co., Inc. v. California*
6 *Cooler, Inc.*, 2 F.3d 1156, at *1 (9th Cir. 1993). As set forth above, § 1798.82 sets forth a
7 geographical limitation that restricts the protections of the CRA to California residents. *See*
8 *Antman*, 2015 WL 6123054, at *5 (“Section 1798.82 has procedures for notifying *California*
9 *residents . . .*” (emphasis added)). Thus, it is no matter whether “the parties [have] stipulate[d]
10 that [the CRA] should apply” to the nationwide class. *Fred Briggs Distributing Co., Inc.*, 2 F.3d
11 at *1 (rejecting argument that non-California plaintiffs could bring a claim under the California
12 Franchise Relations Act, even though the parties stipulated to the application of California law,
13 because “[o]nly franchisees that are domiciled in California” were covered by the California
14 Franchise Relations Act).

15 Plaintiffs cite *Gravquick A/S v. Trimble Navigation Intern. Ltd.*, 323 F.3d 1219, 1222 (9th
16 Cir. 2003), for the proposition that the parties can stipulate to the extraterritorial application of
17 California statutes. In that case, however, the Ninth Circuit concluded that the statute at issue did
18 not limit the statute’s application to only California residents. *See id.* at 1223 (concluding that the
19 California Equipment Dealers Act “include[d] no express requirement limiting its protection to
20 dealers located in California.”). Indeed, the Ninth Circuit in *Gravquick A/S* noted the rule that
21 “[w]hen a law contains geographical limitations on its application . . . courts will not apply it to
22 parties falling outside those limitations, even if the parties stipulate that the law should apply.” *Id.*
23 at 1223. As discussed above, the CRA contains geographical limitations on its application. Thus,
24 Plaintiffs’ reliance on *Gravquick A/S* is not persuasive.

25 Accordingly, the Court GRANTS Defendants’ motion to dismiss the CRA claims of non-
26 California Plaintiffs. Specifically, of the United States Plaintiffs, the Court GRANTS Defendants’
27 motion to dismiss the CRA claims of Plaintiffs Essar, Matthew Ridolfo, Deana Ridolfo, and Garg,
28

1 because these Plaintiffs are not residents of California. *See* CCAC ¶¶ 11–14 (alleging that Essar is
 2 a resident of Colorado, that Matthew Ridolfo and Deana Ridolfo are residents of New Jersey, and
 3 that Garg is a resident of Illinois). This leaves the CRA claims of only United States Plaintiffs
 4 Heines and Dugas, who are California residents. *See* CCAC ¶¶ 10, 12.

5 The Small Business Users Plaintiff, Neff, is a resident of Texas. *Id.* ¶ 20. The Israel
 6 Plaintiffs, Rivlin and Granot, are residents of Israel. CCAC ¶¶ 15–16. Accordingly, the Court
 7 GRANTS Defendants’ motion to dismiss Neff, Rivlin, Granot’s CRA claims.

8 Because Plaintiffs Essar, Matthew Ridolfo, Deana Ridolfo, Garg, Neff, Rivlin, and Granot
 9 are not California residents, they cannot bring a claim under § 1798.82 of the CRA as a matter of
 10 law. Thus, the Court finds that granting these Plaintiffs leave to amend their CRA claim would be
 11 futile, and the Court grants Defendants’ motion to dismiss these Plaintiffs’ CRA claims with
 12 prejudice.⁹

13 The Court next turns to address Defendants’ remaining arguments regarding the CRA
 14 claims of United States Plaintiffs Heines and Dugas.

15 **2. Requirement to Notify about the 2013 Breach**

16 Next, Defendants argue that “CRA notice was not required for California residents
 17 potentially affected by the 2013 Breach” because, at the time of the 2013 Breach, the CRA did not
 18 require Defendants to notify California residents if an unauthorized individual accessed “[a] user
 19 name or email address, in combination with a password or security question and answer that
 20 would permit access to an online account.” *See* Mot. at 32. Defendants’ argument requires

21
 22 ⁹ Plaintiffs state in a footnote that, should the Court find “that non-California Plaintiffs lack
 23 standing to bring a CRA claim, Plaintiffs can amend their Complaint to assert claims, and avail
 24 themselves of remedies, under the security breach notification laws of over a dozen states, and
 25 request leave to do so.” *See* Opp. at 31, n.31. However, to the extent Plaintiffs request leave to
 26 add new claims or new parties, Plaintiffs must file a separate motion for leave to amend and
 27 Plaintiffs must attach a proposed amended complaint to Plaintiffs’ motion. Absent any indication
 28 of what additional “security breach notification” law claims Plaintiffs seek to allege against
 Defendants, or the proposed allegations supporting those claims, the Court cannot determine
 whether granting Plaintiffs leave to amend to add new claims under other security breach
 notification laws would be futile, in bad faith, cause undue delay, or be unduly prejudicial to
 Defendants. *See Leadsinger*, 512 F.3d at 532 (stating that a district court may deny leave to
 amend due to futility, undue delay, bad faith, or undue prejudice to the opposing party).

1 understanding an amendment to the CRA’s definition of “personal information” that became
 2 effective on January 1, 2014. Accordingly, the Court first addresses the CRA’s definition of
 3 “personal information” and the 2014 amendment to that definition. The Court then addresses the
 4 parties’ arguments regarding the 2013 Breach.

5 As set forth above, the CRA establishes procedures for California businesses “to notify
 6 California residents when their unencrypted *personal information* is disclosed in a data breach and
 7 thereby acquired (or reasonably believed to have been acquired by) an unauthorized person.”
 8 *Antman*, 2015 WL 6123054, at *5 (citing Cal. Civ. Code § 1798.82(a)) (emphasis added).
 9 “Personal information” is defined in § 1798.82(h) of the statute. In 2013, at the time of the 2013
 10 Breach, the statute defined personal information as the following:

11 [A]n individual’s first name or first initial and last name, in combination with” at

12 least one or more of the following:

- 13 (1) the individual’s social security number,
- 14 (2) driver’s license number or California identification number,
- 15 (3) account number,
- 16 (4) credit or debit card number, in combination with any required security
 17 code, or password that would permit access to an individual’s financial
 account,
- 18 (5) medical information, and
- 19 (6) health insurance information.

20 *See* RJN, Ex. N. Significantly, the definition of “personal information” in the 2013 version of the
 21 CRA did not include “[a] user name or email address, in combination with a password or security
 22 question and answer that would permit access to an online account.” This language was added to
 23 the definition of “personal information” in § 1798.82(a) by an amendment signed into law on
 24 September 27, 2013, and effective January 1, 2014. *See* RJN, Ex. M (setting forth legislative
 25 history of Senate Bill No. 46, which made amendments to Cal. Civ. Code § 1798.82).

26 Defendants claim that the 2013 Breach revealed only “user name[s] and email address[es]”
 27

1 in combination with . . . password[s] or security question[s] and answer[s].” *Id.* Thus, Defendants
2 argue, the 2013 Breach did not reveal “personal information” as that term was defined in the 2013
3 version of the CRA, and so Defendants were not required to notify Plaintiffs of the 2013 Breach.
4 *See* Mot. at 33–34. Defendants contend that, if the Court were to apply the 2014 amendments to
5 the CRA to Plaintiffs’ CRA claim regarding the 2013 Breach, the Court would be applying the
6 amendments retroactively, which the Court may not do. *Id.*

7 However, Defendants’ argument regarding the timing of the CRA’s application is based on
8 a misinterpretation of the CRA. As set forth above, under the CRA, a California business “that
9 owns or licenses computerized data that includes personal information, shall disclose a breach of
10 the security of the system following discovery or notification of the breach in the security of the
11 data to a resident of California” whose personal information was accessed by an unauthorized
12 individual during the breach. *See* Cal. Civ. Code § 1798.82(a)(2). The statute provides that
13 disclosure of a data breach “shall be made in the most expedient time possible and without
14 unreasonable delay” following discovery of the breach. *Id.* Thus, a business does not violate the
15 CRA simply because a data breach *occurred*. Instead, a business violates the CRA only if the
16 business “discover[s]” or is “notif[ied] of the breach” and thereafter “*unreasonably delay[s]*” in
17 disclosing the data breach. *Id.* (emphasis added). Accordingly, in the instant case, the relevant
18 date for purposes of Plaintiffs’ CRA claim is not the date that the 2013 Breach occurred. Instead,
19 it is the date that Defendants *discovered* the 2013 Breach and thereafter failed to adequately notify
20 Plaintiffs. Thus, as long as Defendants *discovered* the 2013 Breach on January 1, 2014 or later,
21 the 2014 amendment to the CRA applies to Plaintiffs’ CRA claim because Defendants would have
22 violated the CRA in 2014 or later, while the 2014 amendment was in effect.

23 Problematically, however, Plaintiffs’ CCAC does not contain *any* allegations about when
24 Defendants “discover[ed]” or were “notif[ied]” of the 2013 Breach. *Id.* Rather, the CCAC alleges
25 only that Defendants “finally admitted” the 2013 Breach on December 14, 2016. *See* CCAC ¶ 79.
26 Because the CCAC does not allege when Defendants discovered the 2013 Breach, the Court
27 cannot determine which version of the CRA was in effect at the time that Defendants allegedly
28

1 violated the CRA. More significantly, absent any allegations in the CCAC suggesting when
 2 Defendants learned of the 2013 breach, Plaintiffs have not adequately alleged that Defendants
 3 “unreasonably delay[ed]” in notifying Plaintiffs of the 2013 Breach on December 14, 2016. *See*
 4 Cal. Civ. Code § 1798.82(a). Thus, regardless of whether the 2014 amendments to the CRA
 5 apply, Plaintiffs’ allegations regarding the 2013 Breach fail to state a claim under the CRA.¹⁰

6 Thus, the Court GRANTS Defendants’ motion to dismiss Plaintiffs’ CRA claim to the
 7 extent that Plaintiffs’ CRA claim is based on Defendants’ failure to disclose the 2013 Breach. The
 8 Court affords Plaintiffs leave to amend this claim because Plaintiffs may be able to allege facts
 9 sufficient to show that Defendants unreasonably delayed in failing to notify Plaintiffs that the
 10 2013 Breach occurred, and thus leave to amend this claim is not necessarily futile. *See*
 11 *Leadsinger*, 512 F.3d at 532 (holding that leave to amend is proper when amendment is not futile).
 12 The remainder of the Court’s discussion of Plaintiffs’ CRA claim therefore relates only to the
 13 2014 Breach and the Forged Cookie Breach.

14 **3. Requirement to Notify about the Forged Cookie Breach**

15 Next, Defendants argue that the CRA does not apply to the Forged Cookie Breach, which
 16 occurred in 2015 and 2016, because the Forged Cookie breach did “not involve exposure of the
 17 statutory data elements of ‘personal information.’” Mot. at 34. Again, Defendants’ argument is
 18 based on the definition of “personal information” in § 1798.82(h) of the CRA. As set forth above,
 19 the definition of “personal information” in Cal. Civ. Code § 1798.82(h) includes an individual’s
 20 name in combination with one or more of the following data elements: (1) Social Security number;
 21 (2) Driver’s license number or California identification number; (3) Account number or credit or
 22 debit card number, in combination with any required security code, access code, or password that

23
 24 ¹⁰ In a footnote, Plaintiffs assert that even if the 2013 version of the CRA applies to the 2013
 25 Breach, Defendants were nonetheless required to notify Plaintiffs of the 2013 Breach because the
 26 2013 Breach involved the exposure of “personal information” as that term was defined in the 2013
 27 version of the statute. *See* Opp. at 29 n. 28. The Court need not reach this issue because Plaintiffs
 28 have failed to allege that Defendants unreasonably delayed in notifying Plaintiffs of the 2013
 Breach. However, if Plaintiffs can allege unreasonable delay, then the Court would, as with the
 Forged Cookie Breach, likely find that the 2013 Breach exposed personal information as defined
 by the 2013 version of the CRA.

1 would permit access to an individual’s financial account; (4) Medical information; (5) Health
2 insurance information; or (6) Information or data collected through the use or operation of an
3 automated license plate recognition system. *See id.* In addition, effective January 1, 2014, the
4 definition of “personal information” also includes an individual’s “user name or email address, in
5 combination with a password or security question and answer that would permit access to an
6 online account.” *See* Cal. Civ. Code § 1798.82(h).

7 Defendants do not contest that the 2014 Breach involved hackers accessing Plaintiffs’
8 “personal information.” However, in the Forged Cookie Breach, hackers were able to forge
9 authentication cookies, which allowed the hackers to access Plaintiffs’ Yahoo email accounts
10 “without needing to supply the account’s password.” CCAC ¶ 68. Defendants thus argue that,
11 because hackers were able to access Plaintiffs’ accounts without a password, the Forged Cookie
12 Breach did not involve exposure of Plaintiffs’ “user name or email address, in combination with a
13 password or security question and answer that would permit access to an online account,” Cal.
14 Civ. Code § 1798.82(h), and thus did not involve the exposure of Plaintiffs’ “personal
15 information.” Accordingly, Defendants argue they were not required by the CRA to notify
16 Plaintiffs of the Forged Cookie Breach.

17 To resolve this issue, the Court first discusses “cookies,” and then discusses Plaintiffs’
18 allegations regarding the Forged Cookie Breach. The Court then turns to the parties’ arguments.

19 A “cookie” is a small text file that a server creates and sends to a browser, which then
20 stores the file in a particular directory on an individual’s computer.” *In re Facebook Internet*
21 *Tracking Litig.*, 140 F. Supp. 3d 922, 926 (N.D. Cal. Oct. 23, 2015); *see also* CCAC ¶ 67.
22 “[C]ookies contain information about the user’s session with” a particular server. *See* CCAC ¶ 67.
23 “When an individual using a web browser contacts a server—often represented by a particular
24 webpage or internet address—the browser software checks to see if that server has previously set
25 any cookies on the individual’s computer.” *In re Facebook Internet Tracking Litig.*, 140 F. Supp.
26 3d at 926; *see also* CCAC ¶ 67. “If the server recognizes any valid, unexpired cookies, then the
27 computer ‘sends’ those cookies to the server.” *In re Facebook Internet Tracking Litig.*, 140 F.

United States District Court
Northern District of California

1 Supp. 3d at 926. “After examining the information stored in the cookie, the server knows if it is
2 interacting with a computer with which it has interacted before.” *Id.* “Since servers create
3 database records that correspond to individuals, sessions, and browsers, the server can locate the
4 database record that corresponds to the individual, session, or browser using the information from
5 the cookie.” *Id.* Accordingly, cookies allow Yahoo’s servers to recognize a computer that has
6 previously logged in to Yahoo, and thus allow a Yahoo user to revisit the Yahoo website without
7 “need[ing] to log in each time.” CCAC ¶ 67.

8 Plaintiffs allege that, during the Forged Cookie Breach, hackers “were able to forge”
9 authentication cookies, which granted the hackers access to Yahoo users’ email accounts “without
10 needing to supply the account’s password.” CCAC ¶ 68. In addition, “a forged cookie allowed
11 the hackers to remain logged into the hacked accounts for weeks or indefinitely.” *Id.*

12 According to Defendants, because Plaintiffs allege that the Forged Cookie Breach involved
13 users accessing Yahoo accounts “without needing to supply the account’s password,” the Forged
14 Cookie Breach did not involve the hackers gaining unauthorized access to a California resident’s
15 “username or email address, *in combination with* a password or security question and answer that
16 would permit access to an online account.” Cal. Civ. Code § 1798.82(h). Thus, Defendants argue
17 the Forged Cookie Breach did not involve the disclosure of “personal information” of Plaintiffs
18 within the meaning of the CRA, and thus Defendants were not required to notify California
19 residents about the Forged Cookie Breach.

20 Defendants’ argument is not well taken. Plaintiffs allege that hackers forged
21 authentication cookies, which hackers used as a proxy for Plaintiffs’ passwords to gain
22 unauthorized access to California resident’s Yahoo email accounts. *See* CCAC ¶¶ 67–68.
23 Significantly, once hackers gained access to Plaintiffs’ Yahoo email accounts, hackers were able
24 to “remain logged into the hacked accounts for weeks or indefinitely” and access all information
25 contained in the accounts. *Id.* Plaintiffs Heines and Dugas allege that they used their Yahoo email
26 accounts for personal and financial transactions, such as collecting Social Security payments and
27 filing their tax returns. *See* CCAC ¶¶ 10, 12. Indeed, Plaintiffs allege that, in general, users of

1 Yahoo’s email service used their email for numerous sensitive personal and financial purposes.
 2 *See id.* ¶¶ 42–44. Plaintiffs allege that access to an individual’s Yahoo email account could allow
 3 a hacker to access bank accounts, file hosting accounts, personal messages, and other information.
 4 *See id.* Accordingly, even if the Forged Cookie Breach did not involve hackers gaining access to
 5 users’ passwords, Plaintiffs allege that the Forged Cookie Breach nonetheless involved hackers
 6 gaining access to other types of information that § 1798.82(h) defines as “personal information,”
 7 such as “social security number[s],” “medical information,” or “credit or debit card number[s].”
 8 *See* Cal. Civ. Code § 1798.82(h); *see* CCAC ¶¶ 10, 12, 42–44.

9 At the very least, even if Defendants did not *know* that this information was accessed in the
 10 Forged Cookie Breach, based on the allegations in the CCAC, Defendants should have
 11 “*reasonably believed*” that the hackers acquired this information in the Forged Cookie Breach.
 12 *See* Cal. Civ. Code § 1798.82(h) (requiring notification after a business learns that a California
 13 resident’s “personal information was, or is reasonably believed to have been, acquired by an
 14 unauthorized person”). This inference is plausible in light of the fact that Plaintiffs allege that the
 15 Forged Cookie Breach involved prolonged and perhaps *indefinite* access to Plaintiffs’ Yahoo
 16 email accounts and all the information contained in those accounts. *See* CCAC ¶ 68.

17 Thus, even if the Forged Cookie Breach did not involve hackers learning of Plaintiffs’
 18 passwords, Plaintiffs have adequately alleged that the Forged Cookie Breach nonetheless involved
 19 hackers accessing Plaintiffs’ “personal information,” as that information is defined in
 20 § 1798.82(h). Plaintiffs allege that Defendants have admitted in their recent 10-K filing with the
 21 SEC that Defendants knew of the Forged Cookie Breach as it was happening in 2015 and 2016
 22 “but took no real action in the face of that knowledge.” CCAC ¶ 86. Plaintiffs allege that
 23 Defendants “quietly divulged the Forged Cookie Breach in [Defendants’] 10-Q filing with the
 24 SEC filed November 9, 2016,” but that Defendants “declined to notify any affected users at that
 25 time” and indeed did not begin notifying users until “February 2017.” CCAC ¶¶ 80–81. Based on
 26 the CCAC’s allegations, the Court finds that Plaintiffs have adequately alleged that Defendants
 27 “unreasonably delay[ed]” in notifying Plaintiffs that their “personal information” was accessed by

1 unauthorized individuals in the Forged Cookie Breach. *See* Cal. Civ. Code § 1798.82(a).
 2 Accordingly, the Court DENIES Defendants’ motion to dismiss Plaintiffs’ CRA claim based on
 3 the Forged Cookie Breach.

4 **4. Damages from Delayed Notice**

5 Finally, Defendants argue that Plaintiffs’ CRA claim fails because Plaintiffs have not
 6 alleged that their damages flowed from Defendants’ *delay* in notifying Plaintiffs about the Data
 7 Breaches, rather than simply from the Data Breaches themselves. Mot. at 35.

8 As set forth above, § 1798.84 of the CRA, the remedies provision, provides that “[a]ny
 9 customer injured by a violation of this title may institute a civil action to recover damages.” Cal.
 10 Civ. Code § 1798.84(b). “[W]here a plaintiff fails to allege a cognizable injury, the plaintiff ‘lacks
 11 statutory standing’ to bring a claim under § 1798.84, ‘regardless of whether [the] allegations are
 12 sufficient to state a violation of the [statute]’ itself. *In re Adobe*, 66 F. Supp. 3d at 1218; *see also*
 13 *Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, 2016 WL 6523428, at *10 (S.D. Cal. Nov.
 14 3, 2016) (“[P]roof of damages is a threshold hurdle for” a CRA cause of action). To allege a
 15 “cognizable injury” arising from Defendants’ alleged failure to timely notify Plaintiffs of the Data
 16 Breaches, Plaintiffs must allege “incremental harm suffered as a result of the alleged delay in
 17 notification,” as opposed to harm from the Data Breaches themselves. *Dugas*, 2016 WL 6523428,
 18 at *7; *see also In re Sony Gaming Networks*, 996 F. Supp. 2d at 1010 (“[A] plaintiff must allege
 19 actual damages flowing from the unreasonable delay (and not the intrusion itself) in order to
 20 recover actual damages”). Where Plaintiffs have failed to allege injury arising from the
 21 Defendants’ “delayed notification,” courts have dismissed § 1798.82 claims. *See, e.g., Dugas*,
 22 2016 WL 6523428, at *7 (dismissing § 1798.82 claim because Plaintiff did not allege “what, if
 23 any, concrete harm resulted from Defendants’ alleged failure to promptly notify [its] customers of
 24 the data breach”); *In re Sony Gaming Networks*, 996 F. Supp. 2d at 1010 (dismissing § 1798.82
 25 claim where plaintiffs “failed to allege how” a ten-day delay in notification caused plaintiffs’
 26 injuries).

27 According to Defendants, “Plaintiffs have not pled facts showing how they were injured
 28

1 specifically as a result of Defendants’ purported notification delay,” as opposed to the “Data
2 Breaches themselves.” *See* Mot. at 35. The Court disagrees. Plaintiffs allege that, as a result of
3 the 2014 Breach, hackers stole the names, email addresses, recovery email accounts, telephone
4 numbers, birth dates, passwords, security questions and answers, and account “nonces”
5 (cryptographic values unique to each account) of Yahoo account holders, and then “gained access
6 to the email contents of all breached Yahoo accounts and thus any private information contained
7 within those emails,” such as credit card information. *See* CCAC ¶¶ 1, 92. Moreover, once a
8 hacker obtained access to a users’ email account the hacker could then “verify accounts and reset
9 passwords” related to *other* accounts of Yahoo users. As a result of the Forged Cookie Breach,
10 Plaintiffs allege that hackers remained logged into users’ email accounts for “weeks or
11 indefinitely.” *Id.* ¶ 68. As a result of these Data Breaches, Plaintiffs Heines and Dugas
12 experienced fraudulent charges on their accounts and fraudulent tax returns filed in their names,
13 which resulted in harm to their credit scores and hours spent talking to the police, banks, and
14 businesses. *See* CCAC ¶¶ 10, 12. According to the CCAC, Defendants were aware of the 2014
15 Breach as it was occurring in 2014, and yet Defendants did not notify Plaintiffs of the 2014
16 Breach until September 22, 2016, approximately *two years* later. *See* CCAC ¶ 73. Similarly,
17 Plaintiffs allege that Defendants were aware of the Forged Cookie Breach as it was happening in
18 2015–2016, but that Defendants did not inform Plaintiffs of the Forged Cookie Breach until
19 “February 2017,” one to two years later. *See id.* ¶¶ 80–82, 86.¹¹

20 A reasonable inference from these allegations is that if Plaintiffs had been aware of the
21 Data Breaches a year to two years earlier, Plaintiffs could have taken earlier measures to mitigate
22 the harms that they suffered from the Data Breaches. Most significantly, Plaintiffs could have
23 changed their passwords. If Plaintiffs were able to change their passwords following the Data
24 Breaches, the account information stolen during the Data Breaches would be useless to hackers

25
26 ¹¹ As discussed above, Plaintiffs have not alleged when Defendants discovered the 2013 Breach,
27 and thus Plaintiffs have not sufficiently alleged that Defendants unreasonably delayed in notifying
28 users of the 2013 Breach. For the same reason, Plaintiffs have not sufficiently alleged damages
flowing from delay in notification of the 2013 Breach.

United States District Court
Northern District of California

1 because the information would be outdated. Plaintiffs also could have cancelled their Yahoo
2 email accounts entirely. Moreover, even if Plaintiffs could not take these steps immediately, and
3 thus even if hackers did access Plaintiffs’ Yahoo email accounts, Plaintiffs could have taken
4 earlier steps to mitigate the fallout from their information being stolen, such as replacing their
5 credit cards, freezing accounts, or placing credit alerts on their accounts. However, because
6 Defendants delayed in notifying Plaintiffs of the Data Breaches for a year to two years, Plaintiffs
7 could not take these mitigation steps, and thus Plaintiffs have plausibly alleged that they faced
8 incremental harms.

9 Accordingly, the Court finds that Plaintiffs have plausibly alleged incremental damages
10 arising from Defendants’ unreasonable delay in notifying Plaintiffs of the 2014 Breach and the
11 Forged Cookie Breach, as opposed to damages arising from only the Data Breaches themselves.
12 Thus, the Court DENIES Defendants’ motion to dismiss Plaintiffs’ CRA claim for lack of CRA
13 damages.

14 **E. Stored Communications Act**

15 The United States Plaintiffs, Israel Plaintiffs, and Small Business Users Plaintiff allege in
16 Count Four a claim under the federal Stored Communications Act (“SCA”), 18 U.S.C. § 2702.
17 The United States Plaintiffs and the Israel Plaintiffs assert this claim against Yahoo. The Small
18 Business Users Plaintiff asserts this claim against Yahoo and Aabaco, the wholly owned
19 subsidiary of Yahoo that administered Yahoo’s small business services.

20 The SCA provides that “a person or entity providing an electronic communication service
21 to the public shall not knowingly divulge to any person or entity the contents of a communication”
22 that is either stored by the service or is carried by the service “on behalf of and received by means
23 of electronic transmission from . . . a subscriber or customer of the service.” 18 U.S.C.
24 § 2702(a)(1)–(2). Defendants move to dismiss Plaintiffs’ SCA claim on two grounds. First,
25 Defendants argue that Plaintiffs have not sufficiently alleged that Defendants “knowingly
26 divulge[d]” any information. Second, Defendants argue that Plaintiffs have not sufficiently
27 alleged that Defendants divulged the “*contents* of a communication.” *Id.* (emphasis added). For

28

1 the reasons discussed below, the Court finds that Plaintiffs have not sufficiently alleged that
 2 Defendants “knowingly divulge[d]” any information. Thus, the Court need not reach Defendants’
 3 second argument that Plaintiffs have not sufficiently alleged that Defendants divulged the
 4 “contents of a communication.” *Id.*

5 As set forth above, defendant violates the SCA only if the defendant “knowingly
 6 divulge[s]” the contents of certain communications. 18 U.S.C. § 2702(a)(1)–(2). Plaintiffs allege
 7 that “[b]y failing to take commercially reasonable steps to safeguard” Plaintiffs’ communications,
 8 Defendants “knowingly divulged” Plaintiffs’ communications. *See* CCAC ¶¶ 165, 170.

9 The parties have not identified, and the Court is not aware of, any court in the Ninth
 10 Circuit that has addressed the scope of the term “knowingly” in 18 U.S.C. § 2702. However,
 11 courts outside the Ninth Circuit have found that reckless or negligent conduct is insufficient to
 12 constitute “knowing” disclosure of a communication under the SCA, and that plaintiffs
 13 accordingly cannot state claims under the SCA simply because a defendant failed to prevent a data
 14 breach. For example, in *Worix v. MedAssets, Inc.*, 857 F. Supp. 2d 699, 703 (N.D. Ill. 2012), the
 15 court dismissed an SCA claim in a data breach case because “the failure to take reasonable steps to
 16 safeguard data does not, without more, amount to divulging that data knowingly.” Similarly, in
 17 *Willingham v. Glob. Payments, Inc.*, 2013 WL 440702, at *12 (N.D. Ga. Feb. 5, 2013), the court
 18 held that although the plaintiff alleged that the defendant “created or contributed to the breach of
 19 its data system,” such conduct did not constitute “knowingly divulg[ing]” information within the
 20 meaning of the SCA. *See also* *Muskovich v. Crowell*, 1996 WL 707008, at *3 (S.D. Iowa Aug.
 21 30, 1996) (holding that a defendant did not “knowingly divulge” information within the meaning
 22 of the SCA by “failing to implement adequate security procedures to prevent unauthorized access
 23 to the content of electronic information under its control.”). More generally, after analyzing the
 24 statutory text and the legislative history, the Sixth Circuit has held that negligent or recklessness
 25 conduct is insufficient to state an SCA claim. *See Long v. Insight Commc’ns of Cent. Ohio, LLC*,
 26 804 F.3d 791, 795–96 (6th Cir. 2015) (finding Time Warner Cable’s mistaken disclosure of an IP
 27 address was not a violation of the SCA because “negligently or recklessly failing to ensure the
 28

United States District Court
Northern District of California

1 accuracy of the information that [Time Warner Cable] disclosed” did not constitute Time Warner
2 Cable “knowingly divulg[ing] this information” within the meaning of the SCA).

3 Based on the allegations in the CCAC, Plaintiffs have not plausibly alleged that
4 Defendants’ “knowingly divulge[d]” Plaintiffs’ PII in the Data Breaches. As set forth above,
5 Plaintiffs allege only that Defendants “fail[ed] to take commercially reasonable steps” to
6 safeguard” Plaintiffs’ communications. This allegation, without more, does not establish that
7 Defendants “dilvuge[d]” Plaintiffs’ PII and did so with a knowing state of mind. *See* 18 U.S.C.
8 § 2702(a)(1)–(2). Thus, as currently alleged in the CCAC, Plaintiffs have not plausibly alleged
9 that Defendants “knowingly divulg[ed]” Plaintiffs’ information by “failing to take commercially
10 reasonable steps” to safeguard Plaintiffs’ communications. Accordingly, the Court GRANTS
11 Defendants’ motion to dismiss Plaintiffs’ SCA claim. The Court affords leave to amend because
12 amendment may not be futile. *See Leadsinger*, 512 F.3d at 532 (holding that leave to amend is
13 proper when amendment would not be futile).

14 **F. Online Privacy Protection Act**

15 The United States Plaintiffs, Israel Plaintiffs, and the Small Business Users Plaintiff assert
16 a claim in Count Five under the California Online Privacy Protection Act (“OPPA”), Cal. Bus. &
17 Prof. Code § 22575, *et seq.* The United States Plaintiffs and Israel Plaintiffs assert this claim
18 against Yahoo. The Small Business Users Plaintiff asserts this claim against Yahoo and Aabaco.

19 Defendants move to dismiss Plaintiffs’ OPPA claims on three grounds. First, Defendants
20 argue that the OPPA does not provide for a private right of action. Mot. at 37–38. Second,
21 Defendants argue that “Plaintiffs cannot extend that claim beyond California residents.” *Id.* at 38.
22 Third, Defendants argue that the two California residents who assert an OPPA claim Plaintiffs
23 Heines and Dugas, do not qualify as consumers as required under the OPPA. *Id.*

24 Plaintiffs do not contest that Plaintiffs have failed to plead a violation of the OPPA.
25 Specifically, Plaintiffs do not dispute that there is no private right of action under the OPPA, or
26
27

1 that Plaintiffs do not qualify as consumers under the OPPA.¹² Instead of contesting these issues,
 2 Plaintiffs argue that the OPPA “evinces California’s strong public policy of protecting privacy and
 3 customer data,” and that Defendants’ conduct in violation of this “public policy” is actionable
 4 under “the UCL’s unfair prong.” *See* Opp. at 33 (citations omitted).

5 As discussed *supra* in Part III.C, the Court finds that Plaintiffs have adequately alleged a
 6 violation of the unfair prong based on California’s public policy of protecting consumer data.
 7 However, Defendants’ violation of the “public policy” evinced by the OPPA does not justify
 8 bringing a separate cause of action for violation of the OPPA, which Plaintiffs have done here.
 9 Although case law interpreting the OPPA is limited, the California Court of Appeals has explained
 10 that “the OPPA itself does not provide for a private action or public prosecution for any violation
 11 of its provisions.” *People ex rel. Harris v. Delta Air Lines, Inc.*, 247 Cal. App. 4th 884, 891
 12 (2016). Moreover, Plaintiffs do not dispute that the OPPA does not provide Plaintiffs with a
 13 private right of action. Thus, the Court GRANTS Defendants’ motion to dismiss Plaintiffs’ OPPA
 14 claim. This dismissal is with prejudice because, since Plaintiffs lack a private right of action under
 15 the OPPA, the Court finds that amendment of this claim would be futile. *See Leadsinger*, 512 F.3d
 16 at 532 (holding that leave to amend is proper when amendment would not be futile).

17 **G. Express Contract Claim**

18 The United States Plaintiffs, Israel Plaintiffs, and the Small Business Users Plaintiff assert
 19 in Count Six a cause of action for breach of express contract. The United States Plaintiffs and the
 20 Israel Plaintiffs assert this claim against Yahoo. The Small Business Users Plaintiff asserts this
 21 claim against Yahoo and Aabaco.

22 _____
 23 ¹² Plaintiffs fail to respond to Defendants’ argument that the OPPA applies only to California
 24 residents. The Court, however, is not persuaded by Defendants’ argument. In support of their
 25 argument, Defendants note that the OPPA governs “an operator of a commercial Web site or
 26 online service that collects personally identifiable information through the Internet about
 27 individual consumers residing in California who use or visit its commercial Web site.” Cal. Bus.
 28 & Prof. Code § 22575 (emphasis added). However, this provision limits only the *defendants* who
 are subject to the OPPA. It does not appear to limit the *plaintiffs* who can sue for violations by
 these defendants. Defendants cite no other authority in support of their argument. Nevertheless,
 the Court need not resolve this issue because, as discussed above, Plaintiffs’ OPPA claim fails on
 other grounds.

1 Under California law, to state a claim for breach of contract a plaintiff must plead “the
2 contract, plaintiffs’ performance (or excuse for nonperformance), defendant’s breach, and damage
3 to plaintiff therefrom.” *Gautier v. General Tel. Co.*, 234 Cal. App. 2d 302, 305 (1965). To
4 establish contractual damages, a Plaintiff must establish “appreciable and actual damage.”
5 *Aguilera v. Pirelli Armstrong Tire Corp.*, 223 F.3d 1010, 1015 (9th Cir. 2000); *Patent Scaffolding*
6 *Co. v. William Simpson Const. Co.*, 256 Cal. App. 2d 506, 511, 64 Cal. Rptr. 187 (1967) (“A
7 breach of contract without damage is not actionable.”).

8 In the CCAC, Plaintiffs allege that Yahoo breached the following provisions of Yahoo’s
9 Privacy Policy, which is incorporated by reference into Yahoo’s Terms of Service, which form a
10 contract between Yahoo and each user who creates an account with Yahoo:

- 11 • “We are committed to ensuring your information is protected and apply safeguards in
12 accordance with applicable law.”
- 13 • “Yahoo does not rent, sell, or share personal information about you with other people or
14 non-affiliated companies except to provide products or services you’ve requested, when we
15 have your permission, or under [certain inapplicable circumstances].”
- 16 • “We limit access to personal information about you to employees who we reasonably
17 believe need to come into contact with that information to provide products or services to
18 you or in order to do their jobs.”
- 19 • “We have physical, electronic, and procedural safeguards that comply with federal
20 regulations to protect personal information about you.”

21 *See* CCAC ¶ 179. Plaintiffs further allege that Aabaco breached provisions of its Privacy Policy,
22 which is incorporated by reference into Aabaco’s Terms of Service, which form a contract
23 between Aabaco and each user who purchases a service or product from Aabaco. CCAC ¶ 180.
24 Specifically, Plaintiffs allege that Aabaco breached provisions of its Privacy Policy that are
25 substantially identical to the second, third, and fourth provisions in Yahoo’s Privacy Policy,
26 discussed above. *Id.* Accordingly, because the allegedly breached contractual provisions are
27 substantially identical, the Court considers Plaintiffs’ claims against Yahoo and Aabaco together.

1 Plaintiffs allege that Defendants breached the contractual terms discussed above by failing
 2 to have reasonable safeguards in place for protection of Plaintiffs' accounts. Specifically,
 3 Plaintiffs allege that Defendants' "data encryption protocol" had been "widely discredited and had
 4 been proven, many years prior, easy to break." *See, e.g.*, CCAC ¶ 133. Plaintiffs also allege that
 5 Defendants experienced several intrusions, but that "[n]one of these intrusions prompted
 6 [Defendants] to comprehensively review and ameliorate its shoddy security" and that in fact,
 7 Defendants' "internal culture actively discouraged emphasis on data security." *Id.* ¶¶ 50, 52.
 8 Plaintiffs allege that Defendants failed to put reasonable safeguards into place despite having been
 9 "repeatedly put on notice that [Defendants'] security measure were not up to par, leaving users'
 10 PII at risk of theft." *Id.* ¶ 45.

11 Defendants move to dismiss the breach of contract claim on two grounds. First,
 12 Defendants argue that disclaimers contained elsewhere in the Terms of Service demonstrate that
 13 Defendants did not breach the contract. Second, Defendants argue that because of limitations of
 14 liability in the Terms of Service, Plaintiffs cannot establish that they suffered damages from any
 15 breach. The Court considers these arguments in turn.

16 **b. Disclaimers in the Terms of Service**

17 Defendants argue that in claiming that Defendants breached the contractual terms
 18 discussed above, "Plaintiffs grossly mischaracterize Defendants' statements" because "Yahoo and
 19 Aabaco never guaranteed Plaintiffs a completely secure, hack-proof environment." Mot. at 39.
 20 Defendants point to several disclaimers in the Terms of Service that Defendants argue limit
 21 Defendants' obligations under the Terms of Service. Specifically, the Yahoo Terms of Service
 22 state that use of Yahoo services is "AT YOUR OWN RISK" and on an "AS IS" and "AS
 23 AVAILABLE" basis. Moreover, Yahoo's Terms of Service disclaimed warranties that the
 24 services were "UNINTERRUPTED, TIMELY, SECURE OR ERROR-FREE," and warned that
 25 "no data transmission over the Internet or information storage technology can be guaranteed to be
 26 100% secure." *See* Mot. at 39; CCAC, Ex. 1, at 91. Similarly, the Aabaco Terms of Service also
 27 stated that use of Aabaco services was "AT YOUR OWN RISK" and on an "AS IS" and "AS
 28

1 AVAILABLE” basis, disclaimed warranties that the services were “UNINTERRUPTED,
2 TIMELY, SECURE OR ERROR-FREE,” and warned that any “SECURITY MECHANISMS IN
3 THE SERVICES HAVE INHERENT LIMITATIONS.” *Id.*

4 However, contrary to Defendants’ argument, these disclaimers do not absolve Defendants
5 of any contractual obligation to take reasonable steps to protect users’ PII. *See* Mot. at 39–40
6 (arguing that the disclaimers “are the polar opposite of the promises Plaintiffs claim were made”).
7 For example, Defendants’ promised that Defendants “limit access to personal information about
8 you.” *See* CCAC ¶ 179. If this provision means anything, it means that Defendants promised to
9 make reasonable effort to prevent third parties from accessing Plaintiffs’ account information.
10 Indeed, Defendants’ disclaimer that security mechanisms have “inherent limitations” itself implies
11 that there are at least some reasonable security mechanisms in place. *Id.*; *see also In re Adobe Sys.,*
12 *Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1221 (N.D. Cal. 2014) (“Although Adobe contends that
13 there can be no actionable dispute concerning the adequacy of Adobe’s security controls because
14 the Agreement expressly provides that no security measure is “100%” effective, this disclaimer
15 does not relieve Adobe of the responsibility (also contained in the Agreement) to provide
16 “reasonable” security.”) (citations omitted). Thus, at a minimum, Plaintiffs have sufficiently
17 alleged that Defendants violated their promise to “limit access to personal information” about
18 Plaintiffs.

19 Therefore, despite Defendants’ disclaimers, Plaintiffs have pointed to particular provisions
20 of the Terms of Service that Defendants allegedly violated, and Plaintiffs have sufficiently alleged
21 that Defendants violated these provisions by failing to put in place reasonable security measures to
22 protect user data. *See Anthem II*, 2016 WL 3029783, at *10 (“The core message from these
23 documents is the same: to take reasonable security measures to protect customer PII.”). On a
24 motion to dismiss, the Court must accept these allegations “as true and construe the pleadings in
25 the light most favorable to the nonmoving party.” *Manzarek*, 519 F.3d at 1031. For the reasons
26 set forth above, the Court cannot say as a matter of law that Defendants did not breach the
27 contractual terms discussed above simply because Defendants made certain caveats in their

1 Privacy Policies, such as that their services were not “100% secure.”

2 **c. Limitations of Liability in the Terms of Service**

3 Next, Defendants argue that Plaintiffs’ breach of express contract claim fails because
4 Plaintiffs cannot establish damages in light of the limitations of liability in Defendants’ Terms of
5 Service. Specifically, Defendants point out that Yahoo’s Terms of Service contained the
6 following clause limiting Yahoo’s liability:

7 YOU EXPRESSLY UNDERSTAND AND AGREE THAT YAHOO . . . SHALL
8 **NOT BE LIABLE TO YOU FOR ANY PUNITIVE, INDIRECT,**
9 **INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY**
10 **DAMAGES, INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS**
11 **OF PROFITS, GOODWILL, USE, DATA OR OTHER INTANGIBLE LOSSES**
12 **(EVEN IF YAHOO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH**
13 **DAMAGES), RESULTING FROM: . . . UNAUTHORIZED ACCESS TO OR**
14 **ALTERATION OF YOUR TRANSMISSIONS OR DATA . . . OR . . . ANY**
15 **OTHER MATTER RELATING TO THE YAHOO SERVICE.**

16 CCAC, Ex. 1, at 91 (emphasis added). Similarly, Aabaco’s Terms of Service contained the
17 following clause limiting Aabaco’s liability:

18 TO THE MAXIMUM EXTENT ALLOWED BY APPLICABLE LAW, YOU
19 EXPRESSLY UNDERSTAND AND AGREE THAT THE COMPANY . . .
20 **SHALL NOT BE LIABLE, UNDER ANY CIRCUMSTANCES OR LEGAL**
21 **THEORIES WHATSOEVER, FOR ANY INDIRECT, PUNITIVE,**
22 **INCIDENTAL, SPECIAL, CONSEQUENTIAL, OR EXEMPLARY**
23 **DAMAGES**

24 CCAC, Ex. 2, at 172 (emphasis added).

25 Defendants argue that because of these limitation-of-liability clauses, Plaintiffs’ breach of
26 express contract claim must be dismissed because Plaintiffs are not entitled to recover any
27 damages under the breach of express contract claim. However, the plain language of Defendants’
28 Terms of Service limits Defendants’ liability only for “punitive, indirect, incidental, special,
consequential or exemplary damages.” *See* CCAC, Ex. 1, at 91. These limitations of liability
clauses do not limit Defendants’ liability for direct damages. *See id.* In their opposition, Plaintiffs
concede that out-of-pocket mitigation costs are consequential damages. *Opp.* at 35. However,
Plaintiffs claim that all other damages Plaintiffs seek “are direct and non-consequential damages
that flow naturally from Defendants’ breaches of their contractual obligations.” *Id.* Defendants

1 offer no argument regarding which of Plaintiffs' damages are consequential damages, and which
2 of Plaintiffs' damages are direct damages. *See* Mot. at 40–41; Reply at 16.

3 Because the parties agree that Plaintiffs cannot seek consequential damages under
4 Defendants' Terms of Service, and because Plaintiffs concede that out-of-pocket mitigation costs
5 are consequential damages, the Court DISMISSES Plaintiffs' claim for out-of-pocket mitigation
6 damages for Defendants' breach of the Terms of Service. *See* Opp. at 35 (admitting that "out of
7 pocket mitigation costs" are consequential damages). The Court grants leave to amend because
8 Plaintiffs may be able to allege that the limitations in Defendants' Terms of Service are
9 unconscionable,¹³ and thus leave to amend is not necessarily futile. *See Leadsinger*, 512 F.3d at
10 532. The Court otherwise DENIES Defendants' motion to dismiss Plaintiffs' breach of express
11 contract claim. The Court will address the issue of which of Plaintiffs' remaining claims for
12 damages seek direct damages, as opposed to consequential damages, at a later stage of the
13 proceedings when the issue has been properly presented by the parties. *See Mehmet v. Paypal,*
14 *Inc.*, 2009 WL 815676, at *5 (N.D. Cal. Mar. 27, 2009) ("The effect of the limitation of liability
15 clause may very well . . . bar [Plaintiff's] claim . . . but that issue has not been addressed by the
16 parties in a manner sufficient to enable the court to issue such a ruling at this time and is more
17 properly reserved for resolution at a later stage of the proceedings.").

18 **H. Breach of Implied Contract**

19 The United States Plaintiffs, Israel Plaintiffs, and Small Business Users Plaintiff assert in
20 Count Seven a claim against Defendants for breach of implied contract. The United States

21
22 ¹³ In their opposition, Plaintiffs argue that even consequential damages should not be dismissed
23 because Plaintiffs have alleged in their declaratory relief claim that "the limitation of liability
24 language is unconscionable, and thus, unenforceable." Opp. at 35. However, as the Court explains
25 more fully, *infra*, regarding Plaintiffs' declaratory relief claim, Plaintiffs' claim for declaratory
26 relief merely lists various provisions of Yahoo's Terms of Service and alleges that these
27 provisions are "unconscionable and unenforceable, or precluded by federal and state law." CCAC
28 ¶ 234. These "threadbare recitals" that various provisions are unconscionable are insufficient to
state a claim. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) ("Threadbare recitals of the elements of
a cause of action, supported by mere conclusory statements, do not suffice."). Thus, Plaintiffs'
reliance on their conclusory assertion that Defendants' Terms of Service are "unconscionable" is
not sufficient to allege that Defendants' limitations on consequential damages are unconscionable,
and is not sufficient to save Plaintiffs' request for consequential damages here.

1 Plaintiffs and the Israel Plaintiffs assert this claim against Yahoo. The Small Business Users
2 Plaintiff asserts this claim against Yahoo and Aabaco.

3 Defendants argue that Plaintiffs’ implied contract claim is “wholly duplicative of their
4 express contract claim” and that therefore the claim should be dismissed. *See* Mot. at 41.
5 However, the CCAC makes clear that Plaintiffs’ implied contract claim is asserted in the
6 alternative to Plaintiffs’ express contract claim. CCAC ¶ 186 (“To the extent that Defendants’
7 Terms of Service and Privacy Policies did not form express contracts, the opening of a Yahoo or
8 Aabaco account created implied contracts”). Federal Rule of Civil Procedure 8 explicitly
9 allows Plaintiffs to plead different theories of relief in the alternative, even if those theories are
10 inconsistent. Fed. R. Civ. P. 8(d) (“A party may set out 2 or more statements of a claim or defense
11 alternatively or hypothetically A party may state as many separate claims or defenses as it
12 has, regardless of consistency.”). Accordingly, courts routinely allow plaintiffs to plead both
13 express contract and implied contract theories, as long as those theories are clearly pled in the
14 alternative. *See, e.g., SocialApps, LLC v. Zynga, Inc.*, 2012 WL 381216, at *3 (N.D. Cal. Feb. 6,
15 2012) (“While the allegations of the implied contract claim rely on the same allegations as the
16 express contract claim, SA is entitled to plead different theories of recovery in the alternative.”);
17 *Philips Med. Capital, LLC v. Med. Insights Diagnostics Ctr., Inc.*, 471 F. Supp. 2d 1035, 1047
18 (N.D. Cal. 2007) (“Although Counter–Claimants may not ultimately prevail on their claim for
19 [implied contract] if, it turns out, there is a valid express contract between the parties, Counter–
20 Claimants may plead in the alternative.”); *Doe v. John F Kennedy Univ.*, 2013 WL 4565061, at *8
21 (N.D. Cal. Aug. 27, 2013) (“Plaintiff may proceed with alternative claims at the pleading stage,
22 but ultimately [Defendant] cannot be held liable for both breach of express contract and breach of
23 implied contract on the same subject matter.”).¹⁴

24 Defendants’ motion also argues, in a single sentence, that Plaintiffs’ implied contract claim

26 ¹⁴ The only case that Defendants cite in support of their argument, *O’Connor v. Uber Techs., Inc.*,
27 2013 WL 6354534 (N.D. Cal. Dec. 5, 2013), is distinguishable precisely on this basis. In
28 *O’Connor*, there is no indication that the plaintiff had alleged implied contract and express
contract theories in the alternative.

1 should be dismissed because Plaintiffs are required to “elaborate upon the nature and scope of the
2 implied contract in the pleadings, rather than simply declare one existed.” *See* Mot. at 41 (internal
3 quotation marks omitted). However, the CCAC does much more than simply “declare” that an
4 implied contract existed. The CCAC identifies the particular provisions of Defendants’ Terms of
5 Service that allegedly create the implied contract, identifies the conduct that constituted the
6 formation of the implied contract, identifies the terms of the implied contract, and identifies the
7 behavior that allegedly breached the contract. *See* CCAC ¶¶ 185–89 (alleging that an implied
8 contract was created when Plaintiffs opened accounts with Defendants, that the terms of these
9 implied contracts are set forth in the relevant Terms of Service and Privacy Policies, enumerating
10 the terms of the implied contracts, and alleging that Defendants breached these implied contracts
11 because Plaintiffs’ PII was not adequately protected by Defendants). These allegations are
12 sufficient to put Defendants on notice of the nature, source, and terms of the alleged implied
13 contract, and are therefore sufficient to state a claim under Rule 12(b)(6). *See Walters*, 2017 WL
14 1398660, at *2 (“Walters plausibly alleged the existence of an implied contract arising from
15 Kimpton’s privacy policy, which states that Kimpton is ‘committed’ to safeguarding customer
16 privacy and personal information.”).

17 Finally, Defendants argue that, as with Plaintiffs’ express contract claim, Plaintiffs’
18 implied contract claim should be dismissed because of the disclaimers and limitations of liability
19 in Defendants’ Terms of Service. As discussed above, Defendants’ Terms of Service prevents
20 Plaintiffs from recovering consequential damages—such as out-of-pocket mitigation costs, which
21 Plaintiffs concede are consequential—but allows Plaintiffs to recover direct damages. Plaintiffs
22 offer no reason why this conclusion regarding Plaintiffs’ damages for purposes of Plaintiffs’
23 breach of express contract claim does not apply equally to Plaintiffs’ breach of implied contract
24 claim.

25 Thus, as set forth above with regards to Plaintiffs’ breach of express contract claim, the
26 Court DISMISSES Plaintiffs’ claims for out-of-pocket mitigation costs for Defendants’ breach of
27 implied contract. As with the claim for breach of express contract, the Court grants leave to
28

1 amend because Plaintiffs may be able to allege entitlement to consequential damages under the
 2 terms of the alleged implied contract. *See Leadsinger*, 512 F.3d at 532. The Court otherwise
 3 DENIES Defendants’ motion to dismiss Plaintiffs’ breach of implied contract claim, which is
 4 properly pled in the alternative to Plaintiffs’ breach of express contract claim.

5 **I. Implied Covenant of Good Faith and Fair Dealing Claim**

6 The United States Plaintiffs, Israel Plaintiffs, and Small Business Users Plaintiff allege in
 7 Count Eight a claim for breach of the implied covenant of good faith and fair dealing. The United
 8 States Plaintiffs and the Israel Plaintiffs assert this claim against Yahoo. The Small Business
 9 Users Plaintiff asserts this claim against Yahoo and Aabaco.

10 Under California law, “[e]very contract imposes on each party a duty of good faith and fair
 11 dealing in each performance and its enforcement.” *Carson v. Mercury Ins. Co.*, 210 Cal. App. 4th
 12 409, 429 (2012) (internal quotation marks omitted). “The covenant ‘is based on general contract
 13 law and the long-standing rule that neither party will do anything which will injure the right of the
 14 other to receive the benefits of the agreement.’” *Rosenfeld v. JP Morgan Chase Bank, N.A.*, 732
 15 F. Supp. 2d 952, 968 (N.D. Cal. 2010) (quoting *Waller v. Truck Ins. Exchange, Inc.*, 11 Cal. 4th 1,
 16 36 (1995)). In order to establish a breach of the covenant of good faith and fair dealing, a plaintiff
 17 must show: “(1) the parties entered into a contract; (2) the plaintiff fulfilled his obligations under
 18 the contract; (3) any conditions precedent to the defendant's performance occurred; (4) the
 19 defendant unfairly interfered with the plaintiff's rights to receive the benefits of the contract; and
 20 (5) the plaintiff was harmed by the defendant's conduct.” *Id.*

21 Defendants argue that Plaintiffs are attempting to improperly “add terms to [the] express
 22 agreement[.]” and that Plaintiffs have not sufficiently alleged that Defendants exhibited bad faith.
 23 Mot. at 42. The Court addresses these arguments in turn.

24 First, Defendants argue that Plaintiffs have not identified a contractual term that
 25 Defendants violated, but instead have attempted to “impose extra-contractual duties by way of an
 26 implied covenant claim.” *Id.*; see also *Guz v. Bechtel Nat. Inc.*, 24 Cal. 4th 317, 349–50 (2000)
 27 (“It cannot impose substantive duties or limits on the contracting parties beyond those

1 incorporated in the specific terms of their agreement.”). Specifically, Defendants argue that
2 Plaintiffs’ implied covenant claim attempts to “rewrite the contract” to require Defendants to
3 “employ specific password encryption standards; (2) employ specific protocols in cases of
4 suspected or confirmed breaches; (3) employ a particular set of cybersecurity standards; or (4)
5 invest a particular sum of time or money in any ‘cybersecurity resources.’” *Id.* However,
6 Plaintiffs’ implied covenant claim does not impose these “extra-contractual duties.” *Id.* Instead,
7 Plaintiffs’ implied covenant claim relies on the same promises and contractual provisions that
8 Plaintiffs allege Defendants breached in the express contract and implied contract claims. *See*
9 CCAC ¶ 194 (“Defendants . . . breached the implied covenant of good faith and fair dealing with
10 respect to both the specific contractual terms in Yahoo’s Privacy Policy and Aabaco’s Privacy
11 Policy and the implied warranties of their contractual relationships with their users.”); *see also*
12 *Carma Developers (Cal.), Inc. v. Marathon Dev. California, Inc.*, 2 Cal. 4th 342, 373 (1992) (“It
13 is universally recognized the scope of conduct prohibited by the covenant of good faith is
14 circumscribed by the purposes and express terms of the contract.”). As discussed above, Plaintiffs
15 have sufficiently alleged that these contractual terms were violated. Although Defendants did not
16 promise to employ “specific” cybersecurity measures or “invest a particular sum of time or
17 money” in cybersecurity, Plaintiffs have sufficiently alleged that Defendants had a contractual
18 duty to employ reasonable safeguards in protecting users’ PII. Thus, as in the express contract
19 claim and the implied contract claim, the Court finds that Plaintiffs have sufficiently alleged an
20 interference with the benefits of the contract for purposes of Plaintiffs’ claim under the implied
21 covenant of good faith and fair dealing.

22 Next, Defendants argue that Plaintiffs have failed to allege that Defendants exhibited bad
23 faith in violating these contractual duties. Specifically, Defendants claim that Plaintiffs have not
24 alleged a “conscious and deliberate act, which unfairly frustrate[d] the purposes of the parties’
25 written contract.” Mot. at 42; *Hougue v. City of Holtville*, 2008 WL 1925249, at *4 (S.D. Cal.
26 Apr. 30, 2008) (quotations omitted). However, Plaintiffs allege that Defendants “exhibited bad
27 faith through their conscious awareness of and deliberate indifference to the risks to Class

1 members' PII" by failing to take commercially reasonable steps to safeguard Plaintiffs' PII.
2 Taking the allegations in the CCAC as true, as the Court must on a motion to dismiss, Defendants
3 failed to put reasonable safeguards into place despite having been "repeatedly put on notice that
4 [Defendants'] security measure were not up to par, leaving users' PII at risk of theft." *Id.* ¶ 45.
5 Additionally, according to the CCAC, Defendants delayed notifying breached users of the 2014
6 Breach for years, leaving Plaintiffs' PII exposed while Defendants concealed their cybersecurity
7 failures until compelled to do so when Yahoo sought acquisition by Verizon in 2016. *Id.* ¶ 4.
8 Indeed, in a recent 10-K filing with the SEC, Yahoo included a report found several "failures in
9 communication, management, inquiry and internal reporting" relating to the 2014 Breach. *Id.*

10 In short, contrary to Defendants' suggestion, Plaintiffs have not simply alleged that
11 "Defendants engaged in bad faith by failing to assume a host of extra-contractual duties." Instead,
12 Plaintiffs have alleged that Defendants engaged in bad faith by failing to employ minimal
13 reasonable safeguards to protect users' PII in violation of Defendants' contractual duties. Thus,
14 the Court finds that Plaintiffs have adequately alleged a bad faith breach of specific contractual
15 provisions, and therefore the Court finds that Plaintiffs have sufficiently alleged a breach of the
16 implied covenant of good faith and fair dealing. The Court therefore DENIES Defendants' motion
17 to dismiss Plaintiffs' implied covenant of good faith and fair dealing claim.

18 **J. Negligence**

19 The Australia, Venezuela, and Spain Plaintiffs assert in Count Twelve a negligence claim
20 against Yahoo. Defendants move to dismiss this claim on three grounds. First, Defendants argue
21 that the Australia, Venezuela, and Spain Plaintiffs are subject to forum selection clauses that
22 require dismissal. Second, Defendants argue that the negligence claim is barred by the economic
23 loss rule because Plaintiffs have not alleged any physical harm. Third, Defendants argue that the
24 negligence claim should be dismissed on *forum non conveniens* grounds. As set forth below, the
25 Court finds that Plaintiffs' negligence claim is subject to the forum selection clauses and that
26 dismissal is warranted on this basis. Therefore, the Court need not consider Defendants' other
27 arguments. The Court thus turns to address the forum selection clauses.

1 Defendants argue that the Australia, Venezuela, and Spain Plaintiffs cannot assert a
 2 California negligence claim in this Court because the terms of service governing users in those
 3 countries contain forum selection clauses holding that certain foreign laws apply and that claims
 4 can only be brought in those foreign courts. Specifically, Yahoo users are governed by the
 5 “Additional Terms of Service” (“ATOS”), which Yahoo has attached to its request for judicial
 6 notice as Exhibit C. This ATOS first contains several paragraphs that apply to all users
 7 worldwide,¹⁵ followed by several paragraphs detailing particular terms for different geographic
 8 regions. The portion of the ATOS that is specific to Australian users provides as follows:

9 [T]he laws of New South Wales govern not only the interpretation of this ATOS
 10 and apply to claims for breach of it, regardless of conflict of laws principles, but
 11 also apply to all other claims, including claims regarding consumer protection
 12 laws, unfair competition laws, and in tort. You and Yahoo7 Pty Ltd irrevocably
 13 consent to the exclusive jurisdiction and venue of the New South Wales courts for
 14 all disputes arising out of or relating to this ATOS or arising out of or relating to
 15 the relationship between you and Yahoo regardless of the type of claim.

16 RJN, Ex. C, at 10–11. Similarly, the portion of the ATOS that is specific to Venezuela users
 17 provides as follows:

18 [T]he laws of the State of Florida govern not only the interpretation of this ATOS
 19 and applies to claims for breach of it, regardless of conflict of laws principles, but
 20 also applies to all other claims, including claims regarding consumer protection
 21 laws, unfair competition laws, and in tort. You and Yahoo! Hispanic Americas,
 22 LLC irrevocably consent to the exclusive jurisdiction and venue of the courts of
 23 Miami-Dade County for all disputes arising out of or relating to this ATOS or
 24 arising out of or relating to the relationship between you and Yahoo regardless of
 25 the type of claim.

26 RJN, Ex. C, at 6. Finally, the portion of the ATOS that is specific to Spain users provides as
 27 follows:

28 [T]he laws of Ireland govern this ATOS and any non-contractual obligations
 arising out of it. You and YEL [Yahoo! EMEA Limited] irrevocably consent to
 the exclusive jurisdiction and venue of the Irish courts for all disputes arising out
 of or in connection with this ATOS, any non-contractual obligation arising out of
 or in connection with this ATOS or any claim or dispute arising out of or relating

¹⁵ Where these introductory paragraphs are not generally applicable, the ATOS makes this clear. *See, e.g.*, RJN, Ex. C, at 2 (“The prior sentence does not apply to you if you are using the German Services as detailed in Section 10.”).

1 to the relationship between you and YEL regardless of the type of claim.
 2 RJN, Ex. C, at 6. Similar provisions are contained in the “Universal Terms of Service” (UTOS)
 3 specific to each country. *See, e.g.*, RJN, Ex. B, at 1. Defendants argue that Plaintiffs’ negligence
 4 claim against Yahoo in the instant case is sufficiently related to these ATOS, and that therefore the
 5 forum selection clauses in these ATOS should be enforced. Mot. at 45 (internal quotation marks
 6 omitted).

7 In response, Plaintiffs argue that Yahoo cannot take advantage of these forum selection
 8 clauses because *Yahoo* was not a signatory to the ATOS to which Australia, Venezuela, and Spain
 9 users agreed. Instead, as seen in the passages quoted above, the signatories to these contracts were
 10 *Yahoo subsidiaries*: Yahoo7 in the case of Australia, Yahoo! Hispanic Americas in the case of
 11 Venezuela, and Yahoo! EMEA Limited in the case of Spain. *See, e.g.*, RJN, Ex. C, ¶ 3 (“If you are
 12 using the Australian Services, you are contracting with Yahoo7 . . .”).

13 Contrary to Plaintiffs’ argument, the Ninth Circuit has held that “where the alleged
 14 conduct of the nonparties is closely related to” a contract containing forum selection clauses, ““a
 15 range of transaction participants, parties and non-parties, should benefit from and be subject to
 16 forum selection clauses.”” *Holland Am. Line Inc. v. Wartsila N. Am., Inc.*, 485 F.3d 450, 456 (9th
 17 Cir. 2007) (quoting *Manetti–Farrow, Inc. v. Gucci America, Inc.*, 858 F.2d 509, 514 n.5 (9th
 18 Cir.1988)).¹⁶ Thus, the fact that Yahoo is not a party to the foreign ATOS does not alone establish
 19 that Yahoo cannot take advantage of these forum selection clauses contained within those ATOS.
 20 Instead, Yahoo may take advantage of the forum selection clauses contained within the ATOS if
 21 Plaintiffs’ negligence claim against Yahoo “is closely related to the contractual relationship”
 22 between the foreign Plaintiffs and the foreign Yahoo subsidiaries who were signatories to the
 23 foreign terms of service. *Id.*

24 In the instant case, it is clear that Plaintiffs’ negligence claim against Yahoo is closely

25 _____
 26 ¹⁶ Plaintiffs seek leave to file a proposed sur-reply to respond to arguments that Plaintiffs claim
 27 were raised for the first time in Defendants’ reply brief. ECF No. 126. Plaintiffs attach the sur-
 28 reply to the request for leave. ECF No. 126–1. The Court GRANTS this request to file a sur-reply
 and has considered the attached sur-reply in deciding the instant motion to dismiss.

1 related to the ATOS signed by foreign users and the Yahoo subsidiaries providing Yahoo services
2 in those countries. *Id.* Indeed, the ATOS makes extensive references to *Yahoo* itself and
3 describes Yahoo’s obligations and limitations on Yahoo’s liability. For example, the ATOS states
4 that “[y]our registration data and other information about you are also subject to the Yahoo
5 Privacy Policy.” RJN, Ex. C, at 3. The ATOS also contains a disclaimer stating that “Yahoo is
6 not responsible for the security or privacy of communications sent via the Services.” *Id.* at 4.
7 These are just some of the many references to Yahoo and its obligations and liabilities contained
8 in the ATOS governing all users. Additionally, the portions of the ATOS specific to Australia and
9 Venezuela users explicitly state that the forum selection clauses apply to “all disputes arising out
10 of or relating to this ATOS or arising out of or relating to the relationship between you and *Yahoo*
11 regardless of the type of claim.” RJN, Ex. C at 6–11 (emphasis added).

12 The Ninth Circuit’s decision in *Manetti–Farrow, Inc. v. Gucci America, Inc.*, 858 F.2d
13 509, 514 (9th Cir. 1988), is instructive. There, the Manetti-Farrow corporation entered an
14 exclusive dealership contract with Gucci Parfums, but Gucci Parfums later terminated the contract.
15 *Id.* at 510–11. Manetti-Farrow asserted a variety of tort and contract claims against Gucci
16 Parfums and several of its affiliated entities, including Gucci America, which held the American
17 rights to the Gucci trademark. *Id.* at 511. The exclusive dealership contract contained a forum
18 selection clause, but “Manetti–Farrow argue[d] the forum selection clause c[ould] only apply to
19 Gucci Parfums, which was the only defendant to sign the contract.” *Id.* at 514 n.5. The Ninth
20 Circuit rejected this argument and held that “the alleged conduct of the non-parties” in Manetti-
21 Farrow’s tort and contract claims was “so closely related to the contractual relationship [between
22 Manetti-Farrow and Gucci Parfums] that the forum selection clause” in Manetti-Farrow’s contract
23 with Gucci Parfums “applie[d] to all defendants.” *Id.*

24 Similarly, in the instant case, the alleged conduct of Yahoo in the Australia, Venezuela,
25 and Spain Plaintiffs’ negligence claim against Yahoo is “so closely related to the” ATOS between
26 these Plaintiffs and Yahoo’s subsidiaries “that the forum selection clause[s]” in the ATOS apply to
27 Plaintiffs’ negligence claim against Yahoo, even though it is not a party to the ATOS. For

1 example, the CCAC alleges that “Yahoo owed a duty . . . to exercise reasonable care in
 2 safeguarding and protecting the Australia, Venezuela, and Spain Plaintiffs’ PII and financial
 3 information in Yahoo’s possession” CCAC ¶ 225. The Court cannot determine the scope of
 4 Yahoo’s alleged duty to the Australia, Venezuela and Spain Plaintiffs without interpreting
 5 provisions of the ATOS that governed these Plaintiffs’ use of Yahoo services, including
 6 provisions regarding Yahoo’s privacy practices, obligations, liabilities, disclaimers, and other
 7 issues. *See Columbus Univ. v. Tummala*, 2014 WL 12675010, at *4 (C.D. Cal. July 15, 2014)
 8 (holding that a defendant could take advantage of a forum selection clause because the defendant
 9 “was held out to plaintiffs as being a shareholder or manager of” the signatory company).

10 In short, the allegations in the CCAC make clear that the negligence claim against Yahoo
 11 is “closely related” to the contractual relationship between foreign users and Yahoo subsidiaries,
 12 and that the Court must evaluate and “interpret[]” this contractual relationship to resolve
 13 Plaintiffs’ negligence claim. Therefore, applying Ninth Circuit precedent, the Court determines
 14 that Yahoo “should benefit from and be subject to [the] forum-selection clauses.” *TAAG Linhas*
 15 *Aereas de Angola v. Transamerica Airlines, Inc.*, 915 F.2d 1351, 1354 (9th Cir. 1990) (quoting
 16 *Clinton v. Janger*, 583 F. Supp. 284, 290 (N.D. Ill. 1984)). Additionally, Plaintiffs do not argue
 17 that the forum selection clauses were “the product of fraud or overreaching” or that application of
 18 the forum selection clause would be unreasonable for any other reason. *M/S Bremen v. Zapata*
 19 *Off-Shore Co.*, 407 U.S. 1, 15 (1972).

20 Therefore, the Court applies the forum selection clauses governing Australia, Venezuela,
 21 and Spain users and GRANTS Defendants’ motion to dismiss Plaintiffs’ California negligence
 22 claim, which is the only claim asserted by the Australia, Venezuela, and Spain Plaintiffs. Thus,
 23 the Court DISMISSES the Australia, Venezuela, and Spain Plaintiffs. Because these forum
 24 selection clauses forbid the application of California law, Plaintiffs cannot assert their California
 25 negligence claim as a matter of law. Therefore, this dismissal is with prejudice.

26 **K. Declaratory Relief**

27 Finally, all Plaintiffs assert in Count Thirteen a declaratory relief claim against Defendants.

1 ¹⁷ Plaintiffs’ declaratory relief claim alleges that certain provisions of Defendants’ Terms of
 2 Service are “unconscionable and unenforceable, or precluded by federal and state law.” *See, e.g.,*
 3 CACC ¶ 234.

4 Defendants move to dismiss this claim on two grounds. First, Defendants argue that
 5 Plaintiffs have failed to state a claim under Rule 12(b)(6) because Plaintiffs have not sufficiently
 6 alleged that the contractual provisions at issue are unconscionable or otherwise unlawful. Second,
 7 Defendants argue that declaratory relief is improper because it is duplicative of other relief sought
 8 in the CCAC and because the claim merely anticipates an affirmative defense. For the reasons
 9 discussed below, the Court agrees with Defendants that Plaintiffs have not sufficiently alleged that
 10 the contractual provisions at issue are unconscionable or otherwise unenforceable. Thus, the
 11 Court need not reach Defendants’ remaining argument that declaratory relief is improper because
 12 it is duplicative of other relief sought in the CCAC.¹⁸

13 Defendants argue that Plaintiffs’ declaratory relief claim should be dismissed under Rule
 14 12(b)(6). Specifically, Defendants argue that Plaintiffs offer only “threadbare recitals” and “bald
 15 assertions” that the contractual provisions at issue were unconscionable. Mot. at 47. Defendants
 16 also argue that Plaintiffs offer only a “vague allegation that the disputed provisions are ‘precluded’
 17 by unspecified ‘federal and state law.’” Mot. at 48.

18 The Court agrees with Defendants that Plaintiffs’ allegations are insufficient to state a
 19 claim for relief. The CCAC offers no factual allegations at all to support Plaintiffs’ claim for
 20 declaratory relief. Instead, Plaintiffs’ claim for declaratory relief simply lists various provisions of
 21

22 ¹⁷ Although Count Thirteen of the CCAC states that it is brought on behalf of all Plaintiffs, the
 23 CCAC does not explain how the claim for declaratory relief in Count Thirteen is connected to the
 24 Australia, Venezuela, and Spain Class. Additionally, any such claim on behalf of the Australia,
 25 Venezuela, and Spain Class would be foreclosed by the forum selection clauses discussed above in
 26 Part IV.J.

27 ¹⁸ Indeed, as discussed below, because Plaintiffs have failed to plead *any* facts in support of their
 28 claim that Defendants’ Terms of Service are unconscionable or enforceable, the Court cannot
 evaluate at this time whether Plaintiffs’ declaratory relief claim is duplicative, or whether it
 instead “would serve a useful purpose ‘in clarifying and settling the legal relations in issue.’”
McGraw-Edison Co. v. Preformed Line Prod. Co., 362 F.2d 339, 343 (9th Cir. 1966). For this
 additional reason, the Court declines to reach Defendants’ argument that declaratory relief is
 improper in this case.

1 Yahoo’s Terms of Service and alleges that these provisions are “unconscionable and
2 unenforceable, or precluded by federal and state law.” CCAC ¶ 234. The CCAC does not identify
3 the federal and state laws are at issue, and the CCAC does not describe how the listed Terms of
4 Service provisions are unconscionable. *See id.* Additionally, although the declaratory relief claim
5 incorporates the entirety of the CCAC by reference, the CCAC contains no other mention of
6 unconscionability. *See generally* CCAC.

7 Plaintiffs’ allegations are insufficient to state a claim for declaratory relief based on
8 unconscionability and unenforceability. In order to state a claim that a contractual term is
9 unconscionable, Plaintiffs must allege facts showing that the term is “both procedurally and
10 substantively unconscionable.” *In re iPhone Application Litig.*, 2011 WL 4403963, at *7. “The
11 procedural element of unconscionability focuses on two factors: oppression and surprise.” *Id.*
12 (quoting *Aron v. U-Haul Co. of Cal.*, 143 Cal. App. 4th 796, 808 (Cal. Ct. App. 2006)). “The
13 substantive element of unconscionability focuses on the actual terms of the agreement and
14 evaluates whether they create ‘overly harsh’ or ‘one-sided results as to ‘shock the conscience.’”
15 *Id.* The CCAC does not even mention these requirements, let alone plead facts to show that they
16 are met. Instead, the CCAC only offers “threadbare recitals” that various provisions are
17 unconscionable. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (“Threadbare recitals of the elements
18 of a cause of action, supported by mere conclusory statements, do not suffice.”).

19 Similarly, Plaintiffs provide no explanation for their statement that the provisions at issue
20 violate federal or state law, and in fact Plaintiffs do not even indicate which laws these provisions
21 are supposed to have violated. Again, Plaintiffs’ conclusory allegations are not sufficient to defeat
22 a motion to dismiss. *See Davidson v. Apple, Inc.*, 2017 WL 976048, at *13 (N.D. Cal. Mar. 14,
23 2017) (granting motion to dismiss because Plaintiffs did not sufficiently allege unconscionability);
24 *Biggins v. Wells Fargo & Co.*, 266 F.R.D. 399, 412 (N.D. Cal. 2009) (“[T]he claim must be
25 dismissed, because the allegation that ‘the hidden terms . . . are onerous to the point of being
26 unconscionable’ is a bare legal conclusion unsupported by facts.”).

27 Indeed, even in their opposition to the motion to dismiss, Plaintiffs provide little indication
28

United States District Court
Northern District of California

1 of why the cited provisions of Defendants’ Terms of Service are unconscionable or unenforceable.
2 Plaintiffs make no mention in their opposition of the “federal and state laws” that allegedly render
3 Defendants’ Terms of Service unenforceable, and Plaintiffs offer no facts in their opposition
4 demonstrating that Defendants’ Terms of Service are unconscionable. Rather, Plaintiffs make
5 only the conclusory statement that “Plaintiffs submit that the limitation clauses in the [the Terms
6 of Service] are unenforceable. The clauses are both procedurally (clear adhesion contract) and
7 substantively (one-sided and overly harsh) unconscionable.” Opp. at 45. This is not sufficient.

8 In sum, Plaintiffs have failed to adequately allege facts to plausibly suggest that
9 Defendants’ Terms of Service are unconscionable or otherwise unenforceable. Accordingly, the
10 Court GRANTS Defendants’ motion to dismiss Plaintiffs’ claim for declaratory relief. The Court
11 affords Plaintiffs leave to amend because Plaintiffs may be able to sufficiently allege that
12 Defendants’ Terms of Service are unconscionable or otherwise unenforceable, and thus leave to
13 amend this claim is not necessarily futile. *See Leadsinger*, 512 F.3d at 532; *see also Davidson*,
14 2017 WL 976048, at *13 (“Plaintiffs may amend the SACC to allege further facts in support of
15 their unconscionability argument.”).

16 **V. CONCLUSION**

17 For the foregoing reasons, the Court GRANTS IN PART AND DENIES IN PART
18 Defendants’ motion to dismiss. Specifically, the Court rules as follows:

- 19 • The Court DENIES Defendants’ motion to dismiss Plaintiffs’ CCAC for lack of
- 20 Article III standing.
- 21 • The Court GRANTS with leave to amend Defendants’ motion to dismiss the UCL
- 22 claims of Plaintiffs Garg, Rivlin, and Granot. As to the remaining Plaintiffs, the
- 23 Court DENIES Defendants’ motion to dismiss the unlawful and unfair prongs of
- 24 Plaintiffs’ UCL claim. The Court GRANTS with leave to amend Defendants’
- 25 motion to dismiss the fraudulent prong of Plaintiffs’ UCL claim to the extent it is
- 26 based on fraudulent misrepresentations and fraudulent omissions in Defendants’
- 27 Privacy Policy. The Court DENIES Defendants’ motion to dismiss the fraudulent

1 prong of Small Business Plaintiff Neff's UCL claim based on fraudulent omissions
2 in Defendants' Small Business Services advertisements. As to Plaintiffs' request
3 for restitution under the UCL, the Court DENIES Defendants' motion to dismiss
4 Plaintiffs' request for restitution as to Small Business Plaintiff Neff, but GRANTS
5 Defendants' motion to dismiss Plaintiffs' request for restitution for the United
6 States Plaintiffs. The Court DENIES Defendants' motion to dismiss Plaintiffs'
7 request for an injunction under the UCL.

- 8 • The Court GRANTS with leave to amend Defendants' motion to dismiss Plaintiffs'
9 claim for fraudulent inducement.
- 10 • The Court GRANTS with leave to amend Defendants' motion to dismiss Plaintiffs'
11 claim for negligent misrepresentation.
- 12 • The Court GRANTS with leave to amend Defendants' motion to dismiss Plaintiffs'
13 CLRA claim.
- 14 • The Court GRANTS WITH PREJUDICE Defendants' motion to dismiss the CRA
15 claim of Plaintiffs Essar, Matthew Ridolfo, Deana Ridolfo, Garg, Neff, Rivlin, and
16 Granot. As to the remaining Plaintiffs, the Court GRANTS with leave to amend
17 Defendants' motion to dismiss the CRA claim to the extent that the claim is based
18 on the 2013 Breach and DENIES Defendants' motion to dismiss the CRA claim to
19 the extent that the claim is based on the 2014 Breach or the Forged Cookie Breach.
- 20 • The Court GRANTS with leave to amend Defendants' motion to dismiss Plaintiffs'
21 SCA claim.
- 22 • The Court GRANTS WITH PREJUDICE Defendants' motion to dismiss Plaintiffs'
23 OPPA claim.
- 24 • The Court GRANTS with leave to amend Defendants' motion to dismiss Plaintiffs'
25 express contract claim to the extent that the claim seeks to recover out-of-pocket
26 mitigation costs. The Court otherwise DENIES Defendants' motion to dismiss
27 Plaintiffs' express contract claim.

United States District Court
Northern District of California

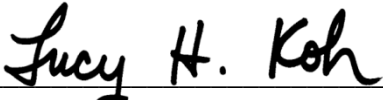
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

- The Court GRANTS with leave to amend Defendants’ motion to dismiss Plaintiffs’ implied contract claim to the extent that the claim seeks to recover out-of-pocket mitigation costs. The Court otherwise DENIES Defendants’ motion to dismiss Plaintiffs’ implied contract claim.
- The Court DENIES Defendants’ motion to dismiss Plaintiffs’ claim for violation of the implied covenant of good faith and fair dealing.
- The Court GRANTS WITH PREJUDICE Defendants’ motion to dismiss Plaintiffs’ negligence claim;
- The Court GRANTS with leave to amend Defendants’ motion to dismiss Plaintiffs’ claim for declaratory relief.

Should Plaintiffs elect to file an amended complaint curing the deficiencies identified herein, Plaintiffs shall do so within 30 days of the date of this Order. Failure to meet the 30 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: August 30, 2017



 LUCY H. KOH
 United States District Judge