

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. 205

Plaintiffs Kimberly Heines, Hashmatullah Essar, Paul Dugas, Matthew Ridolfo, Deana Ridolfo, Yaniv Rivlin, Mali Granot, Brian Neff, and Andrew Mortensen (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’ First Amended Consolidated Class Action Complaint (“FAC”), ECF No. 196. ECF No. 205 (“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**

**A. Factual Background**

1 Defendant Yahoo was founded in 1994 and has since grown into a source for internet  
2 searches, email, shopping, news, and many other internet services. FAC ¶ 32. One of Yahoo’s  
3 most important services is Yahoo Mail, a free email service. *Id.* ¶ 33. Plaintiffs allege that  
4 “[m]any users have built their digital identities around Yahoo Mail, using the service for  
5 everything from their bank and stock trading accounts to photo albums and even medical  
6 information.” *Id.*

7 Yahoo also offers online services for small businesses, including website hosting and email  
8 services (hereinafter, “Small Business Services”). *Id.* ¶ 34. Users must pay for Small Business  
9 Services, and users are required to provide credit or debit card information for automatic monthly  
10 payments for Small Business Services. *Id.* Prior to November 2015, Yahoo provided these  
11 services through a division called Yahoo Small Business. *Id.* “Since November 2015, Yahoo has  
12 provided its small business services through its wholly owned subsidiary Aabaco.” *Id.*

13 Plaintiffs allege that in order to obtain email services and Small Business Services from  
14 Defendants, users are required to provide personal identification information (“PII”) to  
15 Defendants. *Id.* ¶ 35. This PII includes the user’s name, email address, birth date, gender, ZIP  
16 code, occupation, industry, and personal interests. *Id.* ¶ 37. For some Yahoo accounts, including  
17 the small business accounts, users are required to submit additional information, including credit  
18 or debit card numbers and other financial information. *Id.* ¶¶ 34, 36.

19 In addition to the PII that Plaintiffs submitted directly to Defendants, Plaintiffs also allege  
20 that users used their Yahoo email accounts to send and receive a variety of personal information.  
21 *Id.* ¶ 7. Each named Plaintiff alleges that he or she included sensitive information in the content of  
22 his or her Yahoo emails. *See, e.g., id.* ¶¶ 18–21. The individual allegations of the named  
23 Plaintiffs, including allegations regarding the personal information that these named Plaintiffs  
24 included in their Yahoo email accounts, are discussed further below.

### 25 1. Earlier Data Security Issues Putting Yahoo on Notice

26 Plaintiffs allege that Defendants have a long history of data security failures that should  
27 have put Defendants on notice of the need to enhance their data security. For example, in 2008

1 and 2009, “multiple hosts on Yahoo’s corporate network were compromised.” *Id.* ¶¶ 64–65. In  
2 2010, Google notified Yahoo that attackers were using Yahoo systems to attack Google. *Id.* ¶ 66.  
3 In 2011, then-Chief Information Security Officer (“CISO”) Justin Somaini gave a presentation  
4 “identifying gaping holes in Yahoo’s data security.” *Id.* ¶ 67. In 2012, a third party informed  
5 Yahoo of a vulnerability within its system. *Id.* ¶ 72.

6 Yahoo also experienced a breach in 2012. Although the Federal Trade Commission found  
7 as early as 2003 that “SQL injection attacks” were a known and preventable data security threat,  
8 “in 2012, Yahoo admitted that more than 450,000 user accounts were compromised through an  
9 SQL injection attack—with the passwords simply stored in plain text.” *Id.* ¶¶ 77–78. Plaintiffs  
10 allege that according to news stories at the time, “[s]ecurity experts were befuddled . . . as to why  
11 a company as large as Yahoo would fail to cryptographically store the passwords in its database.  
12 Instead, [the passwords] were left in plain text, which means a hacker could easily read them.” *Id.*  
13 ¶ 77.

14 According to Plaintiffs, the 2012 hackers intended the 2012 attack as a wake-up call, and  
15 the hackers left a message stating: “We hope that the parties responsible for managing the security  
16 of this subdomain will take this as a wake-up call, and not as a threat . . . There have been many  
17 security holes exploited in Web servers belonging to Yahoo! Inc. that have caused far greater  
18 damage than our disclosure. Please do not take them lightly.” *Id.* ¶ 79. However, despite this  
19 warning, Plaintiffs allege that “Yahoo’s culture actively discouraged emphasis on data security.”  
20 *Id.* ¶ 89. Plaintiffs allege that “former Yahoo security staffers interviewed later told Reuters that  
21 requests made by Yahoo’s security team for new tools and features such as strengthened  
22 cryptography protections were, at times, rejected on the grounds that the requests would cost too  
23 much money, were too complicated, or were simply too low a priority.” *Id.*

24 Yahoo also hired security firms who identified problems with Yahoo’s systems. For  
25 example, in 2012, Yahoo retained Mandiant, an outside cybersecurity firm, to perform a threat  
26 assessment; Mandiant’s subsequent report detailed issues with Yahoo’s security and attack groups  
27 in Yahoo’s systems. *Id.* ¶¶ 70, 73, 75. Similarly, Dell SecureWorks and Leaf SR conducted  
28

1 security assessments at various times between 2013 and 2016 that turned up vulnerabilities. *Id.*  
 2 ¶¶ 83–84, 87–88.

### 3 **2. Three Data Breaches at Issue in the Instant Case**

4 The instant lawsuit involves three data breaches that occurred between 2013 and 2016.  
 5 According to Plaintiffs, Defendants represented to users that users’ accounts with Defendants were  
 6 secure. For example, Yahoo’s website stated that “protecting our systems and our users’  
 7 information is paramount to ensuring Yahoo users enjoy a secure user experience and maintaining  
 8 our users’ trust” and that “[w]e deploy industry standard physical, technical, and procedural  
 9 safeguards that comply with relevant regulations to protect your personal information.” *Id.* ¶ 43.  
 10 Similarly, Aabaco’s website stated that “[w]e have physical, electronic, and procedural safeguards  
 11 that comply with federal regulations to protect your Personal Information.” *Id.* ¶ 46. Nonetheless,  
 12 despite these representations, Plaintiffs allege that Defendants did not use appropriate safeguards  
 13 to protect users’ PII and that Plaintiffs’ PII was thus exposed to hackers who infiltrated  
 14 Defendants’ systems. Specifically, Plaintiffs allege three separate data breaches: a breach that  
 15 occurred in 2013, a breach that occurred in 2014, and a “forged cookie breach” that occurred in  
 16 2015 and 2016. The Court refers to these breaches collectively as the “Data Breaches.” The  
 17 Court discusses each below.

#### 18 **a. The 2013 Breach**

19 The first breach occurred in August 2013 (“2013 Breach”). *Id.* ¶ 133. Hackers gained  
 20 access to Yahoo accounts and stole users’ Yahoo logins, country codes, recovery emails, dates of  
 21 birth, hashed passwords, cell phone numbers, and zip codes. *Id.* ¶ 134. Significantly, the 2013  
 22 Breach also gave hackers access to the contents of users’ emails, and thus exposed any sensitive  
 23 information that users included in the contents of their emails. *Id.* Plaintiffs allege that users used  
 24 their Yahoo emails for a variety of personal and financial transactions, and thus that Yahoo email  
 25 accounts contained “credit card numbers, . . . bank account numbers, Social Security numbers,  
 26 driver’s license numbers, passport information, birth certificates, deeds, mortgages, and contracts.”  
 27 *Id.*

1 On December 14, 2016, more than three years after the 2013 Breach occurred, Yahoo  
 2 disclosed the 2013 Breach but underestimated its true scope. *Id.* ¶ 133. Specifically, Yahoo stated  
 3 that “an unauthorized third party . . . stole data associated with more than one billion user  
 4 accounts.” *Id.* Almost a year later, on October 3, 2017, Yahoo announced that the 2013 Breach  
 5 had actually affected *every* user account—approximately three billion, not one billion, accounts.  
 6 *Id.* ¶¶ 145–46. Plaintiffs allege that the 2013 Breach occurred because Yahoo did not timely move  
 7 away from an outdated encryption technology known as MD5. *Id.* ¶ 90. According to Plaintiffs, it  
 8 was widely recognized in the data security industry long before the 2013 Breach that MD5 was  
 9 “cryptographically broken and *unsuitable for further use.*” *Id.* ¶ 91. Nevertheless, Yahoo did not  
 10 begin to upgrade from MD5 until the summer of 2013. *Id.* ¶ 93. Plaintiffs allege, however, that  
 11 Yahoo’s move from MD5 in the summer of 2013 was too late to prevent the 2013 Breach. *Id.*  
 12 ¶¶ 94–96.

13 **b. The 2014 Breach**

14 The second breach occurred in late 2014 (“2014 Breach”). *Id.* ¶ 102. Plaintiffs allege that  
 15 “the 2014 breach began with a ‘spear phishing’ email campaign sent to upper-level Yahoo  
 16 employees. One or more of these employees fell for the bait, and Yahoo’s data security was so  
 17 lax, that this action was enough to hand over the proverbial keys to the kingdom.” *Id.* ¶ 154  
 18 (footnote omitted). Through this attack, hackers gained access to at least 500 million Yahoo user  
 19 accounts. *Id.* ¶ 102.

20 According to Plaintiffs, in August 2016, a hacker posted for sale on the dark web the  
 21 personal information of 200 million Yahoo users. *Id.* ¶ 122. Plaintiffs also allege that “a  
 22 geographically dispersed hacking group based in Eastern Europe managed to sell copies of the  
 23 database to three buyers for \$300,000 apiece months before Yahoo disclosed the 2014 Breach.”  
 24 *Id.* ¶ 123.

25 Plaintiffs allege that Yahoo knew about the 2014 Breach as it was happening, but that  
 26 Yahoo did not publicly disclose the existence of the 2014 Breach until September 22, 2016,  
 27 approximately two years later. *Id.* ¶¶ 126, 129. Plaintiffs allege that Yahoo’s announcement of  
 28

1 the 2014 Breach “came just two months after Yahoo announced Verizon’s plan to acquire its  
2 operating assets, and just weeks after Yahoo reported to the SEC that it knew of no incidents of  
3 unauthorized access of personal data that might adversely affect the potential acquisition.” *Id.*  
4 ¶ 126. Plaintiffs allege that Yahoo delayed notifying users or the public about the 2014 Breach  
5 while “Yahoo solicited offers to buy the company. Reportedly, Yahoo wanted the offers in by  
6 April 19, 2016,” and thus waited to disclose the breach until September 2016. *Id.* ¶ 121.

7 Plaintiffs also allege that “[b]y intentionally failing to disclose the breach in a timely  
8 manner as required by law, Yahoo misled consumers into continuing to sign up for Yahoo services  
9 and products, thus providing Yahoo a continuing income stream and a better chance of finalizing a  
10 sale of the company to Verizon.” *Id.* ¶ 130. In the September 22, 2016 announcement of the 2014  
11 Breach, Yahoo stated that the affected “account information may have included names, email  
12 addresses, telephone numbers, dates of birth, hashed passwords (the vast majority with bcrypt)  
13 and, in some cases, encrypted or unencrypted security questions and answers.” *Id.* ¶ 126.

14 Plaintiffs allege that Yahoo’s claim that it had not known about the 2014 Breach for two  
15 years was “met with immediate skepticism.” *Id.* ¶ 128. Indeed, in a 2016 10-K filing with the  
16 SEC, Yahoo revealed that an independent investigation determined that Yahoo had  
17 contemporaneous knowledge of the 2014 Breach, yet failed to properly investigate and analyze the  
18 breach, due in part to “failures in communication, management, inquiry and internal reporting”  
19 that led to a “lack of proper comprehension and handling” of the 2014 Breach. *Id.* ¶ 129.

20 **c. The Forged Cookie Breach**

21 The third data breach occurred sometime in 2015–2016 (“Forged Cookie Breach”). *Id.*  
22 ¶ 117. According to the FAC, the attackers in the Forged Cookie Breach used forged cookies to  
23 access Yahoo users’ accounts. *Id.* “Cookies” are text files that Yahoo places on users’ computers  
24 to store login information so that users do not need to reenter login information every time the  
25 users access their accounts. *Id.* By forging these cookies, hackers were able to access Yahoo  
26 accounts without needing a password to the accounts. *Id.* ¶ 118. Moreover, by forging cookies,  
27 hackers were able to remain logged on to accounts for long periods of time. *Id.*

1 According to Plaintiffs, the attackers in the Forged Cookie Breach are “thought to be the  
2 same parties involved in the 2014 Breach.” *Id.* Specifically, Plaintiffs allege that “the hackers in  
3 the 2014 Breach used some of the data obtained in the 2014 Breach to then forge cookies, help  
4 others forge cookies, or use the cookies to gain actual access to specific accounts.” *Id.* ¶ 119.  
5 “The 2014 Breach and Forged Cookie Breach have since been attributed to two Russian FSB  
6 agents, a Russian hacker, and a Canadian hacker.” *Id.* ¶ 153. Plaintiffs allege that in a 2016 10-K  
7 filing with the SEC, Yahoo disclosed that an independent committee of Yahoo’s Board of  
8 Directors had determined that Yahoo’s information security team knew, at a minimum, about the  
9 Forged Cookie Breach as it was happening, “but took no real action in the face of that  
10 knowledge.” *Id.* ¶ 149. Instead, Plaintiffs allege, Yahoo “quietly divulged” the existence of the  
11 Forged Cookie Breach in Yahoo’s 10-Q filing with the SEC on November 9, 2016 and did not  
12 begin notifying users about the Forged Cookie Breach until February 2017. *Id.* ¶¶ 139, 142.

### 13 3. Allegations of Individual Named Plaintiffs

14 The FAC is brought by nine named Plaintiffs on behalf of four putative classes and one  
15 putative subclass. The Court briefly discusses the allegations of these individual named Plaintiffs  
16 below.

#### 17 a. Named Plaintiffs Representing the United States Class and California Subclass

18 Plaintiffs Kimberly Heines, Hashmatullah Essar, Paul Dugas, Matthew Ridolfo, and Deana  
19 Ridolfo (“United States Plaintiffs”) assert claims on behalf of the putative United States Class,  
20 which consists of all free Yahoo account holders in the United States whose accounts were  
21 compromised in any of the Data Breaches. *Id.* ¶¶ 18–22, 161. Additionally, California Plaintiffs  
22 Heines and Dugas assert claims on behalf of the putative California subclass, which consists of all  
23 California Yahoo account holders whose accounts were compromised in any of the Data Breaches.  
24 *Id.* ¶¶ 18, 20, 163.

25 Plaintiff Kimberly Heines, a resident of California, alleges that she used her Yahoo email  
26 account in conjunction with Direct Express, which is the service through which Plaintiff Heines  
27 receives her Social Security, and thus her Yahoo email account “included . . . information relating

1 to her account with Direct Express.” *Id.* ¶ 18. In 2015, Plaintiff Heines discovered that her  
2 monthly Social Security benefits had been stolen from her Direct Express account and used to  
3 purchase gift cards. *Id.* As a result, Plaintiff Heines fell behind on her bills, and she paid late fees  
4 as a result. *Id.* After the theft, Plaintiff Heines began receiving debt collection calls for debts she  
5 had not herself incurred, and she saw unfamiliar debts on her credit report, which harmed her  
6 credit score. *Id.* Plaintiff Heines alleges that she has spent over 40 hours dealing with the  
7 consequences of the identity theft. *Id.*

8 Plaintiff Hashmatullah Essar, a resident of Colorado, used two free Yahoo email accounts.  
9 *Id.* ¶ 19. Plaintiff Essar used these accounts “for all of his personal, financial, and business needs”  
10 including receiving bank statements, applying for jobs, and securing a mortgage. *Id.* Plaintiff  
11 Essar began receiving “phishing emails from a credit card company purporting to be affiliated  
12 with American Express, asking him to follow a link to log-in to his ‘Serve’ account,” which  
13 Plaintiff Essar did not own. *Id.* After Plaintiff Essar was notified of the 2014 Breach, he signed  
14 up for and has paid \$35.98 per month for LifeLock credit monitoring service. *Id.* In February  
15 2017, “an unauthorized person fraudulently filed a tax return under his Social Security Number,”  
16 and in March 2017 he was denied credit and had freezes placed on his credit. *Id.*

17 Plaintiff Paul Dugas, a resident of California, used four Yahoo email accounts “for his  
18 banking, investment accounts, business emails, and personal emails.” *Id.* ¶ 20. In April 2016,  
19 Plaintiff Dugas was unable to file his personal tax return because a tax return had already been  
20 filed under his Social Security Number. *Id.* As a result, “both of his college-aged daughters  
21 missed deadlines to submit” their financial aid applications, and Plaintiff Dugas was forced to pay  
22 \$9,000 in educational expenses that he otherwise would not have had to pay. *Id.* Moreover,  
23 Plaintiff Dugas has also experienced numerous fraudulent charges on his credit cards, he has had  
24 to replace his credit cards, and he has had to pay money to three different credit bureaus to freeze  
25 his accounts. *Id.*

26 Plaintiffs Matthew Ridolfo and Deana Ridolfo, a married couple, are residents of New  
27 Jersey. *Id.* ¶ 21. They both “used their Yahoo accounts for nearly twenty years for general



1 banking, credit card management and communications, a mortgage refinance, and communication  
 2 with friends and family.” *Id.* Both Plaintiffs Matthew and Deana Ridolfo experienced numerous  
 3 instances of credit card fraud as a result of the Data Breaches. *Id.* Specifically, eleven credit card  
 4 or bank accounts were opened or attempted to be opened in Plaintiff Matthew Ridolfo’s name, and  
 5 at least eight accounts were opened or attempted to be opened in Plaintiff Deana Ridolfo’s name.  
 6 *Id.* The Ridolfos experienced fraudulent charges on their credit cards. *Id.* The Ridolfos  
 7 eventually purchased and enrolled in LifeLock to help monitor their credit and finances, and they  
 8 each pay \$30.00 per month for these services. *Id.* ¶ 22. Nonetheless, as late as January 31, 2017,  
 9 an unauthorized person attempted to open an additional credit card in Plaintiff Deana Ridolfo’s  
 10 name. *Id.*

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

12 Plaintiffs Yaniv Rivlin and Mali Granot (“Israel Plaintiffs”) assert claims on behalf of the  
 13 putative Israel Class, which consists of all Yahoo account holders in Israel whose accounts were  
 14 compromised in any of the Data Breaches. *Id.* ¶¶ 23–24, 161.

15 Plaintiff Yaniv Rivlin, a resident of Tel Aviv, Israel, used his Yahoo email account  
 16 “mainly for personal purposes, including banking, friends and family, credit card statements, and  
 17 social security administration.” *Id.* ¶ 25. Plaintiff Rivlin also pays Yahoo \$20.00 per year for an  
 18 email forwarding service and keeps a credit card on file with Yahoo to pay for the service. *Id.*  
 19 After being notified that his account had been breached, Plaintiff Rivlin has noticed an increase in  
 20 spam and unsolicited advertisements, and Plaintiff Rivlin has spent considerable time changing  
 21 many user names and passwords on many accounts to prevent fraud. *Id.*

22 Plaintiff Mali Granot, a resident of Raanana, Israel, uses her Yahoo email account “to  
 23 correspond with family, friends and school.” *Id.* ¶ 24. Plaintiff Granot was unexpectedly locked  
 24 out of her account and, when she regained access, she received numerous unsolicited chat requests  
 25 and other unsolicited services. *Id.*

26 **c. Named Plaintiff Representing the Small Business Users Class**

27 Plaintiff Brian Neff (“Small Business Users Plaintiff”) asserts claims on behalf of a  
 28

1 putative Small Business Users Class, which consists of all Yahoo or Aabaco business account  
 2 holders in the United States whose accounts were compromised in any of the Data Breaches. *Id.*  
 3 ¶¶ 25–27, 161.

4 Plaintiff Neff, a resident of Texas, “contracted with Yahoo for two services, Yahoo! Web  
 5 Hosting for www.TheInsuranceSuite.com and Yahoo! Business Email, for which he has paid  
 6 Yahoo \$13.94 every month.” *Id.* ¶ 25. Plaintiff Neff has also used Yahoo and Aabaco’s web  
 7 hosting services “in connection with another 54 websites, paying anywhere from \$3.94 to \$15.94  
 8 per month for each website.” *Id.* In May 2015, Plaintiff Neff incurred fraudulent charges on two  
 9 of his credit cards, both of which were on file with Yahoo to pay for the services described above.  
 10 *Id.* ¶ 26. Additionally, a credit card was fraudulently opened in Plaintiff Neff’s name. *Id.*  
 11 Plaintiff Neff has spent “significant time and incurred expenses mitigating the harm to him from  
 12 these security breaches and identity theft.” *Id.* Plaintiff Neff has “stopped using the  
 13 TheInsuranceSuite.com website” and “is in the process of migrating that website to a more secure  
 14 provider,” which Plaintiff Neff alleges will require significant expenses. *Id.* ¶ 27.

15 **d. Named Plaintiff Representing the Paid Users Class**

16 Plaintiff Andrew Mortensen (“Paid Users Plaintiff”) asserts claims on behalf of a putative  
 17 Paid Users Class, which consists of all paid Yahoo account holders in the United States and Israel  
 18 whose accounts were compromised in any of the Data Breaches. *Id.* ¶¶ 28, 161.

19 Plaintiff Mortensen, a resident of Texas, opened an email account with Yahoo and has  
 20 used his account for personal and business purposes, ranging from sharing personal information  
 21 with friends and family to managing banking and financial information. *Id.* ¶ 28. Plaintiff  
 22 Mortensen has also “paid \$19.95 per year for Yahoo’s premium email service.” *Id.* Plaintiff  
 23 Mortensen has received spam calls every week and spam texts every two weeks. *Id.* Plaintiff  
 24 Mortensen alleges that he has been “forced to expend approximately three hours of time and effort  
 25 checking credit and opening accounts.” *Id.*

26 **B. Procedural History**

27 After the 2014 Breach was announced on September 22, 2016, a number of lawsuits were

1 filed against Defendants. These lawsuits generally alleged that Yahoo failed to adequately protect  
2 its users' accounts, failed to disclose its inadequate data security practices, and failed to timely  
3 notify users of the data breach.

4 In late 2016, Plaintiffs in several lawsuits moved to centralize pretrial proceedings in a  
5 single judicial district. *See* 28 U.S.C. § 1407(a) (“When civil actions involving one or more  
6 common questions of fact are pending in different districts, such actions may be transferred to any  
7 district for coordinated or consolidated pretrial proceedings.”). On December 7, 2016, the Judicial  
8 Panel on Multidistrict Litigation (“JPML”) issued a transfer order selecting the undersigned judge  
9 as the transferee court for “coordinated or consolidated pretrial proceedings” in the multidistrict  
10 litigation (“MDL”) arising out of the 2014 Breach. *See* ECF No. 1 at 1–2.

11 On December 14, 2016, one week after the JPML issued the transfer order for cases arising  
12 from the 2014 Breach, Yahoo announced the existence of the 2013 Breach. Plaintiffs in several  
13 lawsuits that had been filed regarding the 2014 Data Breach then amended their complaints to  
14 include claims regarding the 2013 Breach. Additionally, more lawsuits were filed in the Northern  
15 District of California regarding the 2013 Breach and the 2014 Breach. Again, these lawsuits  
16 generally alleged that Yahoo failed to adequately protect its users' accounts, failed to disclose its  
17 inadequate data security practices, and failed to timely notify users of the data breach. These  
18 lawsuits were related or transferred to the undersigned judge. ECF Nos. 7, 9, 30, 33, 40, 64.

19 Plaintiffs filed a Consolidated Class Action Complaint covering all three Data Breaches on  
20 April 12, 2017. ECF No. 80. On May 22, 2017, Defendants filed a first round motion to dismiss.  
21 ECF No. 94. On August 30, 2017, the Court granted in part and denied in part the first round  
22 motion to dismiss. ECF No. 132 (“First MTD Order”).

23 After the Court had issued its ruling on the first round motion to dismiss, Yahoo disclosed  
24 on October 3, 2017 that the 2013 data breach had affected an additional two billion Yahoo user  
25 accounts. In response, the Court amended the case schedule to allow Plaintiffs enough time to  
26 amend their complaint and to conduct discovery. ECF No. 147.

27 Plaintiffs filed the instant FAC on December 15, 2017. ECF No. 174. On January 19,

1 2018, Defendants filed the instant motion to dismiss. ECF No. 205 (“Mot.”). The same day,  
 2 Defendants filed a request for judicial notice in connection with their motion to dismiss. ECF No.  
 3 206. On February 9, 2018, Plaintiffs filed an opposition to Defendants’ motion to dismiss. ECF  
 4 No. 211 (“Opp.”). On February 19, 2018, Defendants filed a reply in support of their motion to  
 5 dismiss. ECF No. 212 (“Reply”).

## 6 **II. LEGAL STANDARD**

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

8 Pursuant to Federal Rule of Civil Procedure 12(b)(6), a defendant may move to dismiss an  
 9 action for failure to allege “enough facts to state a claim to relief that is plausible on its face.” *Bell*  
 10 *Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). “A claim has facial plausibility when the  
 11 plaintiff pleads factual content that allows the court to draw the reasonable inference that the  
 12 defendant is liable for the misconduct alleged. The plausibility standard is not akin to a  
 13 ‘probability requirement,’ but it asks for more than a sheer possibility that a defendant has acted  
 14 unlawfully.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citations omitted).

15 For purposes of ruling on a Rule 12(b)(6) motion, the Court “accept[s] factual allegations  
 16 in the complaint as true and construe[s] the pleadings in the light most favorable to the nonmoving  
 17 party.” *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008).

18 However, a court need not accept as true allegations contradicted by judicially noticeable facts,  
 19 *Shwarz v. United States*, 234 F.3d 428, 435 (9th Cir. 2000), and a “court may look beyond the  
 20 plaintiff’s complaint to matters of public record” without converting the Rule 12(b)(6) motion into  
 21 one for summary judgment, *Shaw v. Hahn*, 56 F.3d 1028, 1029 (9th Cir. 2011). Mere “conclusory  
 22 allegations of law and unwarranted inferences are insufficient to defeat a motion to dismiss.”  
 23 *Adams v. Johnson*, 355 F.3d 1179, 1183 (9th Cir. 2004).

### 24 **B. Leave to Amend**

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

1 of Rule 15 . . . [is] to facilitate decision on the merits, rather than on the pleadings or  
 2 technicalities.” *Lopez v. Smith*, 203 F.3d 1122, 1127 (9th Cir. 2000) (citation omitted).  
 3 Nonetheless, a district court may deny leave to amend a complaint due to “undue delay, bad faith  
 4 or dilatory motive on the part of the movant, repeated failure to cure deficiencies by amendments  
 5 previously allowed, undue prejudice to the opposing party by virtue of allowance of the  
 6 amendment, [and] futility of amendment.” *See Leadsinger, Inc. v. BMG Music Publ’g*, 512 F.3d  
 7 522, 532 (9th Cir. 2008) (alteration in original) (citation omitted).

### 8 **III. REQUEST FOR JUDICIAL NOTICE**

9 The Court first addresses Defendants’ request for judicial notice. ECF No. 206. The Court  
 10 may take judicial notice of matters that are either “generally known within the trial court’s  
 11 territorial jurisdiction” or “can be accurately and readily determined from sources whose accuracy  
 12 cannot reasonably be questioned.” Fed. R. Evid. 201(b). Public records, including judgments and  
 13 other publicly filed documents, are proper subjects of judicial notice. *See, e.g., United States v.*  
 14 *Black*, 482 F.3d 1035, 1041 (9th Cir. 2007) (“[Courts] may take notice of proceedings in other  
 15 courts, both within and without the federal judicial system, if those proceedings have a direct  
 16 relation to matters at issue.”); *Rothman v. Gregor*, 220 F.3d 81, 92 (2d Cir. 2000) (taking judicial  
 17 notice of a filed complaint as a public record).

18 However, to the extent any facts in documents subject to judicial notice are subject to  
 19 reasonable dispute, the Court will not take judicial notice of those facts. *See Lee v. City of L.A.*,  
 20 250 F.3d 668, 689 (9th Cir. 2001) (“A court may take judicial notice of matters of public record  
 21 . . . . But a court may not take judicial notice of a fact that is subject to reasonable dispute.”  
 22 (internal quotation marks and citation omitted)), *overruled on other grounds by Galbraith v. Cty.*  
 23 *of Santa Clara*, 307 F.3d 1119 (9th Cir. 2002).

24 Defendants request judicial notice of the following documents:

25 Ex. A: Legislative Counsel’s Digest for California Assembly Bill 1541;

26 Ex. B: California Assembly, Committee on Privacy and Consumer Protection, Analysis of  
 27 Assembly Bill 1541.

1 Plaintiffs do not object to Defendants' request for judicial notice. The Court agrees that  
 2 these documents are proper subjects of judicial notice. *See Anderson v. Holder*, 673 F.3d 1089,  
 3 1094 n.1 (9th Cir. 2012) ("Legislative history is properly a subject of judicial notice."). Therefore,  
 4 the Court GRANTS Defendants' unopposed request for judicial notice of Exhibits A and B. The  
 5 Court next turns to address the substance of Defendants' motion to dismiss the FAC.

#### 6 **IV. DISCUSSION**

7 As set forth above, the United States Plaintiffs assert claims on behalf of the putative  
 8 United States Class, which consists of all free Yahoo account holders in the United States whose  
 9 accounts were compromised in any of the Data Breaches. FAC ¶¶ 18–22, 161. Additionally, the  
 10 California Plaintiffs assert claims on behalf of the putative California subclass, which consists of  
 11 all California Yahoo account holders whose accounts were compromised in any of the Data  
 12 Breaches. *Id.* ¶¶ 18, 20, 163.

13 The Israel Plaintiffs assert claims on behalf of the putative Israel Class, which consists of  
 14 all Yahoo account holders in Israel whose accounts were compromised in any of the Data  
 15 Breaches. *Id.* ¶¶ 23–24, 161.

16 The Small Business Users Plaintiff asserts claims on behalf of a putative Small Business  
 17 Users Class, which consists of all Yahoo or Aabaco business account holders in the United States  
 18 whose accounts were compromised in any of the Data Breaches. *Id.* ¶¶ 25–27, 161.

19 The Paid Users Plaintiff asserts claims on behalf of a putative Paid Users Class, which  
 20 consists of all paid Yahoo account holders in the United States and Israel whose accounts were  
 21 compromised in any of the Data Breaches. *Id.* ¶¶ 28, 161.

22 The FAC asserts a total of thirteen causes of action: six California statutory claims and  
 23 seven California common-law claims on behalf of the putative classes. Specifically, the FAC  
 24 asserts the following thirteen causes of action: (1) a claim under the unlawful prong of the  
 25 California Unfair Competition Law ("UCL") on behalf of all classes (Count One); (2) a claim  
 26 under the unfair prong of the UCL on behalf of all classes (Count Two); (3) a claim for deceit by  
 27 concealment on behalf of all classes (Count Three); (4) a claim for negligence on behalf of all

1 classes (Count Four); (5) a claim for breach of contract on behalf of all classes (Count Five); (6) a  
 2 claim for breach of implied contract on behalf of all classes (Count Six); (7) a claim for breach of  
 3 the implied covenant of good faith and fair dealing on behalf of all classes (Count Seven); (8) a  
 4 claim for declaratory relief on behalf of all classes (Count Eight); (9) a claim under the fraudulent  
 5 prong of the UCL on behalf of the Small Business Users Class (Count Nine); (10) a claim for  
 6 misrepresentation on behalf of the Small Business Users Class (Count Ten); (11) a claim under the  
 7 California Consumers Legal Remedies Act (“CLRA”) on behalf of the Paid Users Class (Count  
 8 Eleven); (12) a claim under § 1798.81.5 of the California Customer Records Act (“CRA”) on  
 9 behalf of the California subclass (Count Twelve); and (13) a claim under § 1798.82 of the CRA on  
 10 behalf of the California subclass (Count Thirteen). *Id.* ¶¶ 180–312.

11 Defendants move to dismiss claims that were either dismissed with leave to amend in the  
 12 First MTD Order or were newly added in the FAC. First, Defendants raise particular objections to  
 13 eleven of Plaintiffs’ thirteen causes of action—i.e., all claims except the claim under the  
 14 fraudulent prong of the UCL on behalf of the Small Business Users Class (Count Nine) and the  
 15 claim for misrepresentation on behalf of the Small Business Users Class (Count Ten). Next,  
 16 Defendants argue that Plaintiffs may not seek punitive damages as to any of their claims.

17 The Court first considers Defendants’ challenges to Plaintiffs’ causes of action in turn,  
 18 then considers Defendants’ arguments regarding punitive damages.

19 **A. UCL**

20 In Count One, all Plaintiffs allege a claim under the unlawful prong of the UCL. In Count  
 21 Two, all Plaintiffs allege a claim under the unfair prong of the UCL. Defendants move to dismiss  
 22 the UCL unlawful and unfair claims of Plaintiffs Rivlin, Granot, and Mortensen on the ground that  
 23 those three Plaintiffs lack standing to bring claims under the UCL. Mot. at 5–6.

24 In order to establish standing for a UCL claim, Plaintiffs must show that they personally  
 25 “lost money or property as a result of the unfair competition.” Cal. Bus. & Prof. Code § 17204;  
 26 *Kwikset Corp. v. Superior Court*, 246 P.3d 877, 887 (Cal. 2011). As the California Supreme Court  
 27 has explained:

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

9 *Kwikset*, 246 P.3d at 885–86.

10           Under those standards, this Court previously dismissed the UCL claims of Plaintiffs Rivlin  
11 and Granot because they did not sufficiently allege standing under the UCL. First MTD Order at  
12 39. The Court explained that “Plaintiffs’ imminent risk of *future* costs as a result of the Data  
13 Breaches . . . is not sufficient to allege ‘lost money or property’ under the UCL.” *Id.*

14           Plaintiffs Rivlin and Granot’s amended allegations fare no better. Again, the FAC states  
15 that “the Yahoo Data Breaches have caused [Plaintiffs Rivlin and Granot] to be at substantial risk  
16 for identity theft, if in fact [their] identit[ies] ha[ve] not already been stolen.” FAC ¶¶ 23–24. As  
17 the Court has already concluded, such reliance on the threat of future harm does not satisfy the  
18 UCL’s “lost money or property” standing requirement. Indeed, Plaintiffs concede that, based on  
19 the Court’s prior ruling, the UCL claims of Plaintiffs Rivlin and Granot cannot proceed. *Opp.* at 4  
20 n.6. Thus, the Court GRANTS Defendants’ motion to dismiss the UCL unlawful and unfair  
21 claims of Plaintiffs Rivlin and Granot. The Court dismisses with prejudice because Plaintiffs  
22 Rivlin and Granot have failed to cure the deficiencies addressed in the First MTD Order.

23           The Court reaches a different conclusion as to Paid Users Plaintiff Mortensen. To the  
24 extent that Plaintiff Mortensen claims a “greater risk of identity theft and other fraud,” FAC ¶ 28,  
25 like Plaintiffs Rivlin and Granot, he has failed to allege “lost money or property” under the UCL.  
26 However, Plaintiff Mortensen offers further allegations beyond those of Plaintiffs Rivlin and  
27 Granot. Plaintiffs argue that these allegations establish standing under the UCL because he has  
28 alleged lost benefit of the bargain. *Opp.* at 4. The Court agrees.

          Plaintiff Mortensen’s allegations are sufficient to allege that he suffered benefit-of-the-  
bargain losses. In particular, Plaintiff Mortensen pleads that he has paid \$19.95 each year since



1 December 2007 for Yahoo’s premium email service. FAC ¶ 28. Defendants represented that their  
2 email services were “secure.” *Id.* ¶ 40. Plaintiff Mortensen alleges that he “would not have  
3 provided [his] PII to Yahoo or signed up for the supposedly secure services” had he known that  
4 Yahoo’s email service was not as secure as Defendants represented. *Id.* ¶ 285. Accordingly,  
5 Plaintiff Mortensen claims that he was damaged because he paid for services “either worth nothing  
6 or worth less than was paid for them because of their lack of security.” *Id.* ¶ 210. These  
7 allegations closely parallel the Small Business Users Plaintiff Neff’s allegations, which the Court  
8 concluded adequately alleged lost benefit of the bargain. First MTD Order at 36–37.

9 Defendants’ central response is that Plaintiff Mortensen does not allege that he was  
10 deprived of the premium services for which he paid. Mot. at 6. In other words, Defendants argue  
11 that because added security was not a benefit of Plaintiff Mortensen’s bargain with Defendants,  
12 Plaintiff Mortensen has failed to allege lost benefit of the bargain. Reply at 3.

13 Based on Plaintiff Mortensen’s specific allegations, the Court rejects Defendants’  
14 argument in this context. Plaintiff Mortensen’s request for lost benefit of the bargain mirrors the  
15 California Supreme Court’s determination in *Kwikset* that a plaintiff who has “surrender[ed] in a  
16 transaction more, or acquire[d] in a transaction less, than he or she otherwise would have” may  
17 bring a UCL claim. 246 P.3d at 885. Plaintiff Mortensen’s allegations state that he expected to  
18 receive secure email services and that he would not have signed up for the services in the absence  
19 of such assurances. FAC ¶ 285. Even if his annual fee did not provide for security measures  
20 above and beyond those for free accounts, Plaintiff Mortensen pleads that Defendants’  
21 representations about security formed part of the reason for him to use Yahoo Mail in the first  
22 place and to pay \$19.95 per year for the premium email service. *Id.* Moreover, Plaintiff  
23 Mortensen alleges that he would not have signed up for the supposedly secure services or turned  
24 over his PII at all if Defendants had disclosed the security issues. *Id.* Defendants’ argument does  
25 not undermine Plaintiff Mortensen’s plausible allegations that he lost the benefit of the bargain.

26 Such benefit-of-the-bargain losses are sufficient to allege “lost money or property,” and  
27 thus standing, under the UCL. *See In re Anthem, Inc. Data Breach Litig.*, No. 15-MD-02617-

1 LHK, 2016 WL 3029783, at \*30 (N.D. Cal. May 27, 2016) (finding plaintiffs’ alleged benefit of  
 2 the bargain losses were sufficient to establish standing under the UCL); *In re Adobe Sys., Inc.*  
 3 *Privacy Litig.*, 66 F. Supp. 3d 1197, 1224 (N.D. Cal. 2014) (finding allegations that plaintiffs  
 4 “personally spent more on Adobe products than they would had they known Adobe was not  
 5 providing the reasonable security Adobe represented it was providing” to be sufficient to allege  
 6 standing under the UCL). Accordingly, Paid Users Plaintiff Mortensen has adequately alleged  
 7 standing under the UCL, and the Court DENIES Defendants’ motion to dismiss Plaintiff  
 8 Mortensen’s UCL unlawful and unfair claims for lack of UCL standing.

9 **B. Deceit by Concealment and Negligence**

10 All Plaintiffs bring a claim for deceit by concealment in Count Three and a claim for  
 11 negligence in Count Four. Defendants first argue that the economic loss rule bars both sets of  
 12 claims. Mot. at 22–24. Defendants separately contend that, with respect to the deceit by  
 13 concealment claim, Plaintiffs have failed to plead either reliance or damages. Id. at 19–22. The  
 14 Court addresses each of these arguments in turn.

15 **1. Economic Loss Rule**

16 Defendants first contend that Plaintiffs’ deceit by concealment and negligence claims fail  
 17 under the economic loss rule. Mot. at 22–24.

18 Under the economic loss rule, “purely economic losses are not recoverable in tort.” *NuCal*  
 19 *Foods, Inc. v. Quality Egg LLC*, 918 F. Supp. 2d 1023, 1028 (E.D. Cal. 2013) (citing *S.M. Wilson*  
 20 *& Co. v. Smith Int’l, Inc.*, 587 F.2d 1363, 1376 (9th Cir. 1978)); *Robinson Helicopter Co. v. Dana*  
 21 *Corp.*, 102 P.3d 268, 272 (Cal. 2004) (“The economic loss rule requires a purchaser to recover in  
 22 contract for purely economic loss due to disappointed expectations, unless he can demonstrate  
 23 harm above and beyond a broken contractual promise.”). The purpose of the rule is to “prevent[ ]  
 24 the law of contract and the law of tort from dissolving one into the other.” *Robinson Helicopter*,  
 25 102 P.3d at 273 (citation omitted); *Aas v. Superior Court*, 12 P.3d 1125, 1135 (Cal. 2000) (“A  
 26 person may not ordinarily recover in tort for the breach of duties that merely restate contractual  
 27 obligations.”), *superseded by statute on other grounds as recognized in McMillin Albany LLC v.*

1 *Superior Court*, 408 P.3d 797 (Cal. 2018). However, the economic loss rule does not prevent  
 2 recovery in tort if a “special relationship” exists between the plaintiff and the defendant. *J’Aire*  
 3 *Corp. v. Gregory*, 598 P.2d 60, 63 (Cal. 1979); *Biakanja v. Irving*, 320 P.2d 16, 19 (Cal. 1958).

4 Although Defendants argue that the “special relationship” exception never applies when  
 5 the plaintiff and the defendant are in privity, Mot. at 23, this Court has previously rejected that  
 6 argument. As the Court explained, “[w]hen determining whether a special relationship exists  
 7 under *J’aire* between parties that are in privity of contract, California courts have drawn a  
 8 distinction between contracts involving goods and contracts involving services.” *R Power*  
 9 *Biofuels, LLC v. Chemex LLC*, No. 16-CV-00716-LHK, 2016 WL 6663002, at \*5 (N.D. Cal. Nov.  
 10 11, 2016). Specifically, the California Court of Appeal’s decision in *North American Chemical*  
 11 *Co. v. Superior Court* held that where parties are in privity of contract, the *J’aire* exception applies  
 12 if the contracts are for services. 69 Cal. Rptr. 2d 466, 477 (Ct. App. 1997). Other courts in this  
 13 district have reached the same conclusion. *See, e.g., Corelogic, Inc. v. Zurich Am. Ins. Co.*, No.  
 14 15-CV-03081-RS, 2016 WL 4698902, at \*5 (N.D. Cal. Sept. 8, 2016). Thus, the crucial issue for  
 15 applying the *J’aire* exception here is whether the contract at issue is one for goods or services. *R*  
 16 *Power Biofuels*, 2016 WL 6663002, at \*7.

17 The allegations in the FAC counsel that the contract between Plaintiffs and Defendants is  
 18 one for services, not goods. A contract for “goods” involves the purchase or sale of “all things . . .  
 19 which are movable at the time of identification to the contract for sale,” Cal. Com. Code  
 20 § 2105(1), while a contract for services involves the purchase of labor and the “knowledge, skill,  
 21 and ability” of the contracting party. *TK Power, Inc. v. Textron, Inc.*, 433 F. Supp. 2d 1058, 1062  
 22 (N.D. Cal. 2006). Here, Plaintiffs plead that Defendants provided email and other related services  
 23 by maintaining a web-based platform where users can set up accounts. FAC ¶¶ 33–34. Not only  
 24 does the FAC repeatedly refer to what Defendants provide as “services,” *see, e.g., id.* ¶¶ 24–28,  
 25 30, 32, 173, but Defendants themselves have Terms of Service, which state that “Yahoo! provides  
 26 the Yahoo! Services,” *id.*, Ex. 1, at 1. Thus, Plaintiffs’ contract with Defendants is properly  
 27 characterized as a contract for services.

1 Having concluded that the contract is for services, the *J'aire* exception is available to  
 2 Plaintiffs if they have adequately pled a “special relationship.” The *J'aire* court utilized six  
 3 factors for determining when a “special relationship” exists:

4 (1) the extent to which the transaction was intended to affect the plaintiff, (2) the  
 5 foreseeability of harm to the plaintiff, (3) the degree of certainty that the plaintiff  
 6 suffered injury, (4) the closeness of the connection between the defendant’s  
 7 conduct and the injury suffered, (5) the moral blame attached to the defendant’s  
 8 conduct and (6) the policy of preventing future harm.

9 598 P.2d at 63. Applying these criteria to the facts as pled, it is evident that a duty was owed by  
 10 Defendants to Plaintiffs in the present case.

11 First, the contract entered into between the parties related to email services for Plaintiffs.  
 12 Plaintiffs were required to turn over their PII to Defendants and did so with the understanding that  
 13 Defendants would adequately protect Plaintiffs’ PII and inform Plaintiffs of breaches. FAC ¶ 215.  
 14 Second, it was plainly foreseeable that Plaintiffs would suffer injury if Defendants did not  
 15 adequately protect the PII. *Id.* Third, the FAC asserts that hackers were able to gain access to the  
 16 PII and that Defendants did not promptly notify Plaintiffs, thereby causing injury to Plaintiffs.  
 17 *See, e.g.*, ¶ 221. Fourth, the injury was allegedly suffered exactly because Defendants provided  
 18 inadequate security and knew that their system was insufficient. *Id.* ¶ 215. Fifth, Defendants  
 19 “knew their data security was inadequate” and that “they [did not] have the tools to detect and  
 20 document intrusions or exfiltration of PII.” *Id.* “Defendants are morally culpable, given their  
 21 repeated security breaches, wholly inadequate safeguards, and refusal to notify Plaintiffs . . . of  
 22 breaches or security vulnerabilities.” *Id.* Sixth, and finally, Defendants’ concealment of their  
 23 knowledge and failure to adequately protect Plaintiffs’ PII implicates the consumer data protection  
 24 concerns expressed in California statutes, such as the CRA and CLRA. *See In re Adobe Sys.*, 66  
 25 F. Supp. 3d at 1227.

26 Although Defendants seek to short-circuit this analysis by referring to general  
 27 propositions, Mot. at 23–24, the Ninth Circuit has admonished district courts for failing to  
 28 examine all of *J'aire*’s six factors. *Kalitta Air, L.L.C. v. Cent. Tex. Airborne Sys., Inc.*, 315 F.

United States District Court  
Northern District of California

1 App’x 603, 606 (9th Cir. 2008). Under those factors, Plaintiffs have adequately pled a “special  
2 relationship” with Defendants, so Plaintiffs’ negligence and deceit by concealment claims are not  
3 barred by the economic-loss rule. Because Defendants make no other arguments with respect to  
4 the negligence claim, the Court DENIES Defendants’ motion to dismiss Plaintiffs’ negligence  
5 claim.

6 Defendants make additional arguments for dismissal of the deceit by concealment claim.  
7 Specifically, Defendants contend that Plaintiffs’ deceit by concealment claim fails to plead either  
8 reliance or damages. The Court therefore turns to these remaining arguments.

9 **2. Deceit by Concealment**

10 Under California law, a plaintiff may assert a claim for deceit by concealment based on  
11 “[t]he suppression of a fact, by one who is bound to disclose it, or who gives information of other  
12 facts which are likely to mislead for want of communication of that fact.” Cal. Civ. Code  
13 § 1710(3). An action for fraud and deceit based on concealment has five elements:

- 14 (1) the defendant must have concealed or suppressed a material fact, (2) the
- 15 defendant must have been under a duty to disclose the fact to the plaintiff, (3) the
- 16 defendant must have intentionally concealed or suppressed the fact with the intent
- 17 to defraud the plaintiff, (4) the plaintiff must have been unaware of the fact and
- 18 would not have acted as he did if he had known of the concealed or suppressed
- 19 fact, and (5) as a result of the concealment or suppression of the fact, the plaintiff
- 20 must have sustained damage.

21 *Tenet Healthsystem Desert, Inc. v. Blue Cross of Cal.*, 199 Cal. Rptr. 3d 901, 920 (Ct. App. 2016)  
22 (quoting *Mktg. W., Inc. v. Sanyo Fisher (USA) Corp.*, 7 Cal. Rptr. 2d 859, 864 (Ct. App. 1992)).

23 Defendants challenge only the last two elements, contending that Plaintiffs fail to sufficiently  
24 plead reliance or damages in connection with their deceit by concealment claims. Mot. at 19–22.

25 The Court addresses each of these arguments in turn.

26 **i. Reliance**

27 Defendants first contend that the deceit by concealment claims of all Plaintiffs (except  
28 Plaintiff Neff) must be dismissed because there is no allegation that any Plaintiff read Yahoo’s  
Privacy Policy when signing up for a Yahoo Mail account. Mot. at 19–20. The Court disagrees.

1 As noted above, under the reliance element, the plaintiff must demonstrate that he “would  
2 not have acted as he did if he had known of the concealed or suppressed fact.” *Tenet*  
3 *Healthsystem*, 199 Cal. Rptr. 3d at 920 (quoting *Mktg. W.*, 7 Cal. Rptr. 2d at 864). Plaintiffs’  
4 allegations satisfy that requirement. Plaintiffs allege that Defendants knew that their system was  
5 vulnerable to attack by at least 2012 and learned of the 2014 Breach while it was happening. FAC  
6 ¶ 201. In spite of this knowledge, Defendants did not warn Plaintiffs about the security problems  
7 or the 2014 Breach. *Id.* ¶¶ 202–04, 207. The FAC highlights the importance of Defendants’  
8 security measures as a factor in Plaintiffs’ decision whether to use Defendants’ services. *See, e.g.,*  
9 *id.* ¶¶ 184, 191, 205–06. Finally, Plaintiffs explain that, had they known about the inadequacy of  
10 these security measures, they “would have taken measures to protect themselves.” *Id.* ¶ 205.  
11 Plaintiffs’ allegations are sufficient to show that they would have behaved differently had  
12 Defendants disclosed the security weaknesses of the Yahoo Mail system.

13 The sole argument raised in Defendants’ motion to dismiss is unpersuasive. Harkening  
14 back to the dismissal of Plaintiffs’ UCL fraud claim in this Court’s First MTD Order, Defendants  
15 argue that Plaintiffs do not plead that they read Yahoo’s Privacy Policy. Mot. at 19–20.  
16 Defendants’ reliance on this portion of the First MTD Order is misplaced. The Court required  
17 Plaintiffs to plead that they actually read and relied on the Privacy Policy because Plaintiffs’  
18 theory was that Defendants made misrepresentations in the Privacy Policy. First MTD Order at  
19 48–49. Here, in contrast, Plaintiffs’ deceit by concealment claim is not based on statements in the  
20 Privacy Policy, so whether Plaintiffs read the Privacy Policy is immaterial.

21 Perhaps sensing this deficiency, Defendants do not repeat the same argument in their reply  
22 but instead raise two new contentions. Even if the Court were to consider these belated assertions,  
23 they are unavailing. *See Pham v. Fin. Indus. Regulatory Auth. Inc.*, No. 12-CV-06374-EMC, 2013  
24 WL 1320635, at \*1 (N.D. Cal. Apr. 1, 2013) (“[T]hese arguments—raised for the first time on  
25 reply—have been waived.”), *aff’d sub nom. Huy Pham v. Fin. Indus. Regulatory Auth., Inc.*, 589  
26 F. App’x 345 (9th Cir. 2014). First, Defendants argue that Plaintiffs must provide more detail  
27 about Defendants’ omissions, Reply at 11–12, but they offer no explanation of what more

1 Plaintiffs need to identify, and the Court finds that what Plaintiffs have identified is sufficiently  
2 specific.

3 Second, Defendants also criticize Plaintiffs for continuing to use Yahoo Mail and taking no  
4 remedial actions after learning of Defendants' allegedly inadequate security. *Id.* at 12. However,  
5 Defendants fail to acknowledge that Defendants' delayed disclosures are likely to have harmed  
6 Plaintiffs in the interim. Plaintiffs did not even know that they should take any remedial actions  
7 during the periods of Defendants' delayed disclosures. Moreover, contrary to Defendants'  
8 suggestion, the actions that Plaintiffs took after the fact do not conclusively determine what  
9 actions they would have taken if they had been alerted before the fact. The FAC provides at least  
10 one good reason why Plaintiffs may not have ceased their use of Yahoo Mail after the fact—  
11 namely, Plaintiffs have already established their “digital identities around Yahoo Mail.” FAC  
12 ¶ 33. Plaintiffs can consistently plead that they took minimal or no action after learning of the  
13 security defects but that they “would have taken measures to protect themselves” if they had been  
14 informed beforehand. *Id.* ¶ 205. Accordingly, Plaintiffs have plausibly alleged the necessary  
15 element of reliance.

## 16 ii. Damages

17 Defendants argue that, except for Plaintiff Neff, Plaintiffs do not properly plead damages  
18 from the concealment. Mot. at 21. Specifically, Defendants contend that Plaintiffs are limited to  
19 recovering out-of-pocket losses. *Id.* at 20. The out-of-pocket measure is designed to put the  
20 plaintiff in the financial position he or she was in prior to the transaction. *All. Mortg. Co. v.*  
21 *Rothwell*, 900 P.2d 601, 609 (Cal. 1995). Under that measure, Defendants contend, Plaintiffs with  
22 free Yahoo accounts have suffered no damage because they did not pay anything to use Yahoo  
23 Mail. Mot. at 21.

24 In arguing that Plaintiffs are limited to out-of-pocket losses, Defendants rely on California  
25 Civil Code § 3343. Section 3343(a) states that “[o]ne defrauded in the purchase, sale or exchange  
26 of property is entitled to recover the difference between the actual value of that with which the  
27 defrauded person parted and the actual value of that which he received.” In other words, in

1 § 3343(a), the California legislature has expressly provided that the out-of-pocket measure is  
2 applicable in fraud cases involving the “purchase, sale or exchange of property.” *All. Mortg.*, 900  
3 P.2d at 609 (quoting Cal. Civ. Code § 3343(a)). The question in the instant case is whether  
4 § 3343(a) governs Plaintiffs’ deceit by concealment claims. It does not.

5 By its terms, § 3343(a) is restricted to cases where the plaintiff is “defrauded in the  
6 purchase, sale or exchange of property.” The same limitation appears in the title of the statutory  
7 section: “Fraud in purchase, sale or exchange of property; additional damages.” Defendants’ cited  
8 California state authorities follow that pattern. In *Alliance Mortgage*, the plaintiff claimed fraud in  
9 the inducement of a loan for the purchase of real property. 900 P.2d at 605. In *Fladeboe v.*  
10 *American Isuzu Motors Inc.*, the plaintiff alleged fraud and negligent misrepresentation in  
11 connection with the sale of automobiles. 58 Cal. Rptr. 3d 225, 233 (Ct. App. 2007). Moreover, in  
12 all of Defendants’ district court cases, the underlying fraud claim was based in contract. *See Song*  
13 *Fi, Inc. v. Google, Inc.*, No. 14-CV-05080-CW, 2016 WL 1298999, at \*7 (N.D. Cal. Apr. 4, 2016)  
14 (concerning fraud claim where plaintiffs alleged that defendants had duty to disclose based on the  
15 Terms of Service contract between the parties); *Daly v. Viacom, Inc.*, 238 F. Supp. 2d 1118, 1125  
16 (N.D. Cal. 2002) (concerning fraud claim where “plaintiff allege[d] that defendant misrepresented  
17 material facts when it induced plaintiff to sign a contract”).

18 This case is different, as no exchange of property occurred and Plaintiffs’ claim does not  
19 sound in contract. FAC ¶¶ 200–11. Rather, Plaintiffs allege that Defendants committed deceit by  
20 concealment under California Civil Code § 1709 by violating the duty to disclose. The California  
21 Court of Appeal has ruled that, for the tort of deceit, “the appropriate measure of damages is  
22 defined by Civil Code sections 1709 and 3333.” *Sprague v. Frank J. Sanders Lincoln Mercury,*  
23 *Inc.*, 174 Cal. Rptr. 608, 610 (Ct. App. 1981); *see also Romo v. Stewart Title of Cal.*, 42 Cal. Rptr.  
24 2d 414, 422 (Ct. App. 1995) (“A tort victim is not limited to his or her ‘out-of-pocket’ losses;  
25 rather, he or she is entitled to compensatory damages for any actual loss, as well as punitive  
26 damages for fraud (if the fraud consisted of an intentional misrepresentation or concealment).”).  
27 Neither of those statutes is limited to out-of-pocket losses. California Civil Code § 1709 permits



1 recovery of “any damage which [the plaintiff] thereby suffers.” Similarly, California Civil Code  
 2 § 3333 instructs that “[f]or the breach of an obligation not arising from contract, the measure of  
 3 damages . . . is the amount which will compensate for all the detriment proximately caused  
 4 thereby, whether it could have been anticipated or not.” Thus, the out-of-pocket restriction in  
 5 § 3343 does not apply, and Plaintiffs are entitled to recover their compensatory damages.

6 Accordingly, the Court DENIES Defendants’ motion to dismiss Plaintiffs’ deceit by  
 7 concealment claim.

### 8 **C. Contract Claims**

9 In Counts Five through Seven, all Plaintiffs assert contract claims against Defendants.  
 10 Specifically, Plaintiffs assert breach of contract in Count Five, breach of implied contract in Count  
 11 Six, and breach of the implied covenant of good faith and fair dealing in Count Seven. Defendants  
 12 move to dismiss these claims to the extent that they seek consequential damages in light of the  
 13 limitations of liability in Defendants’ Terms of Service. Mot. at 6–7. Plaintiffs argue that they  
 14 have adequately pled that Defendants’ limitation-of-liability provisions are unconscionable. Opp.  
 15 at 5–12. Alternatively, Plaintiffs argue that their claims seek direct damages from Defendants’  
 16 breach of contractual obligations. *Id.* at 13–14. Because the Court agrees that Plaintiffs have  
 17 adequately pled unconscionability, the Court need not address Plaintiffs’ alternative argument.

18 Defendants argue that their Terms of Service bar recovery for damages other than direct  
 19 damages. Specifically, Defendants point out that Yahoo’s Terms of Service contained the  
 20 following clause limiting Yahoo’s liability:

21 **YOU EXPRESSLY UNDERSTAND AND AGREE THAT YAHOO! . . .**  
 22 **SHALL NOT BE LIABLE TO YOU FOR ANY PUNITIVE, INDIRECT,**  
 23 **INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY**  
 24 **DAMAGES, INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS**  
 25 **OF PROFITS, GOODWILL, USE, DATA OR OTHER INTANGIBLE LOSSES**  
 26 **(EVEN IF YAHOO! HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH**  
**DAMAGES), RESULTING FROM: . . . UNAUTHORIZED ACCESS TO OR**  
**ALTERATION OF YOUR TRANSMISSIONS OR DATA . . . OR . . . ANY**  
**OTHER MATTER RELATING TO THE YAHOO! SERVICE.**

27 FAC, Ex. 1, at 10 (emphasis added). Aabaco’s Terms of Service contained the same clause

1 limiting Aabaco’s liability. *Id.*, Ex. 16, at 17. Plaintiffs argue that these limitations of liability are  
 2 unconscionable. *Opp.* at 5–12.

3 In order to state a claim that a contractual term is unconscionable, Plaintiffs must allege  
 4 facts showing that the term is both procedurally and substantively unconscionable. *Pokorny v.*  
 5 *Quixtar, Inc.*, 601 F.3d 987, 996 (9th Cir. 2010); *In re iPhone Application Litig.*, No. 11-MD-  
 6 02250-LHK, 2011 WL 4403963, at \*7 (N.D. Cal. Sept. 20, 2011). “The procedural element of  
 7 unconscionability focuses on two factors: oppression and surprise.” *Aron v. U-Haul Co. of Cal.*,  
 8 49 Cal. Rptr. 3d 555, 564 (Ct. App. 2006). “The substantive element of unconscionability focuses  
 9 on the actual terms of the agreement and evaluates whether they create overly harsh or one-sided  
 10 results as to shock the conscience.” *Id.* (internal quotation marks and citation omitted). Although  
 11 unconscionability is ultimately a question of law, “numerous factual inquiries bear upon that  
 12 question.” *A & M Produce Co. v. FMC Corp.*, 186 Cal. Rptr. 114, 123 (Ct. App. 1982).

13 Plaintiffs have adequately alleged oppression and surprise to support procedural  
 14 unconscionability. “Oppression arises from an inequality of bargaining power which results in no  
 15 real negotiation and an absence of meaningful choice.” *Id.* at 122 (internal quotation marks and  
 16 citation omitted). “Surprise involves the extent to which the supposedly agreed-upon terms of the  
 17 bargain are hidden in a prolix printed form drafted by the party seeking to enforce the disputed  
 18 terms.” *Id.* (internal quotation marks omitted). The Ninth Circuit has held that “a contract is  
 19 procedurally unconscionable under California law if it is ‘a standardized contract, drafted by the  
 20 party of superior bargaining strength, that relegates to the subscribing party only the opportunity to  
 21 adhere to the contract or reject it.’” *Pokorny*, 601 F.3d at 996 (quoting *Ting v. AT&T*, 319 F.3d  
 22 1126, 1148 (9th Cir. 2003)). Plaintiffs plead such a circumstance in alleging that Defendants’  
 23 liability limitations appear near the end of the 12-page legal Terms of Service document where the  
 24 Terms of Service are contained in an adhesion contract and customers may not negotiate or  
 25 modify any terms. FAC ¶¶ 236–37. Although the fact that Plaintiffs could have used other email  
 26 services may weaken their procedural unconscionability claim, the Ninth Circuit has “consistently  
 27 followed the [California] courts that reject the notion that the existence of ‘marketplace  
 28

1 alternatives’ bars a finding of procedural unconscionability.” *Shroyer v. New Cingular Wireless*  
 2 *Servs., Inc.*, 498 F.3d 976, 985 (9th Cir. 2007).<sup>1</sup>

3 Under the particular circumstances of this case, Plaintiffs have also made sufficient  
 4 allegations to support substantive unconscionability. In particular, Plaintiffs claim that the  
 5 limitations of liability are overly one-sided and bar any effective relief. FAC ¶¶ 238, 240. In  
 6 *Silicon Valley Self Direct, LLC v. Paychex, Inc.*, the court found substantively unconscionable a  
 7 nearly identical provision that “exempt[ed] under all circumstances ‘special, indirect, incidental, or  
 8 consequential or punitive damages, including any theory of liability (including contract, tort or  
 9 warranty).” No. 15-CV-01055-EJD, 2015 WL 4452373, at \*6 (N.D. Cal. July 20, 2015). Like  
 10 the provision at issue in *Silicon Valley*, Defendants’ limitations of liability here involve  
 11 “expansive liability limitation and preclusion of nearly every type of damages claim.” *Id.*  
 12 California courts have similarly concluded that limitations are substantively unconscionable when  
 13 they “guarantee[] that plaintiffs could not possibly obtain anything approaching full recompense  
 14 for their harm.” *Lhotka v. Geographic Expeditions, Inc.*, 104 Cal. Rptr. 3d 844, 852 (Ct. App.  
 15 2010); *see also Harper v. Ultimo*, 7 Cal. Rptr. 3d 418, 423 (Ct. App. 2003) (finding substantive  
 16 unconscionability where the damages limitation at issue did not even allow for “the theoretical  
 17 possibility [that the customer] can be made whole”).

18 Defendants suggest that their limitations of liability are not so broad. For example, they  
 19 point out that there is no bar on direct damages. Mot. at 12. Nevertheless, the same was true in  
 20 *Silicon Valley*. Moreover, Plaintiffs further support this point by pleading that “[c]onsequential  
 21 damages are . . . a clear and well-understood consequence of a data breach.” FAC ¶ 240. That  
 22 allegation further supports Plaintiffs’ argument that consequential damages are imperative to  
 23

---

24 <sup>1</sup> Defendants also argue that California courts agree “that contracts for nonessential recreational  
 25 activities cannot be procedurally unconscionable.” *Pokrass v. The DirecTV Grp., Inc.*, No. 07-  
 26 CV-00423-VAP, 2008 WL 2897084, at \*7 (C.D. Cal. July 14, 2008). Defendants do not,  
 27 however, explain how email qualifies as a recreational activity. In fact, the FAC highlights how  
 28 users have “built their digital identities around Yahoo Mail,” using the service for banking, stock  
 trading, and medical information. FAC ¶¶ 7, 33. Additionally, the Small Business Users Class  
 uses the system for conducting business. *Id.* ¶ 34.

1 address the injuries from Defendants’ inadequate security. Additionally, substantive  
2 unconscionability is not defeated by Defendants’ promise not to invoke the limitations against  
3 certain of Plaintiffs’ claims in this case. Mot. at 12. The substantive unconscionability inquiry  
4 looks to whether the *actual terms* of the agreement create overly harsh or one-sided results. *Aron*,  
5 49 Cal. Rptr. 3d at 564. Here, Defendants do not point to any language in their limitations of  
6 liability that restricts their scope. Hence, the actual terms of the limitations of liability allow  
7 Defendants to evade important California common-law and statutory obligations, such as the CRA  
8 and CLRA. FAC ¶ 242.

9 Finally, Plaintiffs make allegations about the lack of a reasonable commercial justification  
10 for Defendants’ limitations on liability. Plaintiffs point out that “Defendants have obligations  
11 under both state and federal law to maintain acceptable levels of data security” and are better-  
12 equipped to bear the risk as “technology giants providing internet services which they advertised  
13 as being safe and sophisticated.” *Id.* ¶ 239. In contrast, individual users “who just want to sign up  
14 for an email address” are not as well-situated to shoulder such risks. *Id.* ¶ 240. In this way,  
15 Plaintiffs conclude that the limitations’ allocation of risk is unreasonable and unexpected. *See id.*  
16 (alleging a “commercially unfair re-allocation of risk”). To be sure, when a defendant offers a free  
17 service, it may be commercially reasonable for the defendant to “retain broad discretion over those  
18 services and to minimize its exposure to monetary damages.” *Darnaa, LLC v. Google, Inc.*, No.  
19 15-CV-03221-RMW, 2015 WL 7753406, at \*3 (N.D. Cal. Dec. 2, 2015). However, especially in  
20 light of the allegations that Defendants took minimal action despite knowing about their  
21 inadequate security measures, Plaintiffs adequately plead that Defendants’ limitations of liability  
22 are substantively unconscionable.

23 In sum, Plaintiffs have adequately pled the necessary elements of procedural and  
24 substantive unconscionability. Accordingly, the Court DENIES Defendants’ motion to dismiss  
25 Plaintiffs’ claims for breach of contract, breach of implied contract, and breach of the implied  
26 covenant of good faith and fair dealing.

27 **D. Declaratory Relief**

1 All Plaintiffs assert in Count Eight a claim for declaratory relief against Defendants.  
2 Plaintiffs' declaratory relief claim alleges that certain provisions of Defendants' Terms of Service  
3 are "unconscionable and unenforceable, or precluded by federal and state law." FAC ¶ 257.

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. Mot. at  
7 15. Second, Defendants argue that declaratory relief is improper because it is duplicative of other  
8 relief sought in the FAC. *Id.* Because the Court has already concluded that Plaintiffs have  
9 sufficiently alleged unconscionability, the Court need only address Defendants' second argument  
10 that Plaintiffs' declaratory relief claim is redundant of Plaintiffs' contract claims.

11 Under 28 U.S.C. § 2201(a), "any court of the United States, upon the filing of an  
12 appropriate pleading, may declare the rights and other legal relations of any interested party  
13 seeking such declaration, whether or not further relief is or could be sought." A claim for  
14 declaratory relief may be "unnecessary where an adequate remedy exists under some other cause  
15 of action." *Reyes v. Nationstar Mortg. LLC*, No. 15-CV-01109-LHK, 2015 WL 4554377, at \*7  
16 (N.D. Cal. July 28, 2015) (quoting *Mangindin v. Wash. Mut. Bank*, 637 F. Supp. 2d 700, 707  
17 (N.D. Cal. 2009)). However, "[t]he existence of another adequate remedy does not preclude a  
18 declaratory judgment that is otherwise appropriate." Fed. R. Civ. P. 57. Ultimately, a critical  
19 question is whether the declaratory relief "will serve a useful purpose in clarifying and settling the  
20 legal relations in issue." *McGraw-Edison Co. v. Preformed Line Prods. Co.*, 362 F.2d 339, 342  
21 (9th Cir. 1966).

22 Defendants point out that Plaintiffs' declaratory relief claim borrows the unconscionability  
23 allegations from Plaintiffs' contract claims. FAC ¶ 258. Defendants argue that because "Plaintiffs  
24 allege no additional facts or otherwise meaningfully differentiate the contract and declaratory  
25 relief claims," the declaratory relief claim is "wholly redundant." Mot. at 15. Plaintiffs respond  
26 that the contract and declaratory relief claims are distinct. While the contract claims seek "past  
27 damages" for Defendants' conduct, the declaratory relief claim seeks "a forward-looking

1 declaration” of the unenforceability of provisions in Defendants’ Terms of Service. Opp. at 17.  
2 The Court concludes that the declaratory relief claim may move forward.

3 Based on the pleadings, the contract claims and the declaratory relief claim seek different  
4 relief. The contract claims request retrospective relief—namely, damages—for the past harms that  
5 Plaintiffs have suffered as a result of Defendants’ failure to keep their promises about adequate  
6 security. FAC ¶¶ 243, 247, 254. In contrast, the declaratory relief claim asks the Court to declare  
7 that certain provisions of Defendants’ Terms of Service are unconscionable. *Id.* ¶ 257. Although  
8 Plaintiffs’ contract claims are similarly premised on claims that those provisions are  
9 unconscionable, those arguments are merely a means to obtaining damages for the harms already  
10 suffered. A declaration of unconscionability would govern ongoing interactions between  
11 Plaintiffs and Defendants and clarify the parties’ legal rights under the Terms of Service.  
12 Therefore, the Court concludes that Plaintiffs’ declaratory relief claim appears to serve a distinct  
13 purpose from the contract claims and thus should not be dismissed.

14 Other courts have allowed plaintiffs to pursue declaratory relief in similar circumstances  
15 when such relief is premised on other viable claims. *See, e.g., In re Easysaver Rewards Litig.*, 737  
16 F. Supp. 2d 1159, 1175 (S.D. Cal. 2010); *California v. Kinder Morgan Energy Partners, L.P.*, 569  
17 F. Supp. 2d 1073, 1091 (S.D. Cal. 2008). Indeed, one case from outside this district noted the  
18 distinction between forward-looking and retrospective relief in concluding that the plaintiff could  
19 maintain its declaratory relief claim with its breach of contract claim. *Kenneth F. Hackett &*  
20 *Assocs., Inc. v. GE Capital Info. Tech. Sols., Inc.*, 744 F. Supp. 2d 1305, 1311 (S.D. Fla. 2010).  
21 Many of Defendants’ cited authorities are inapposite. For example, in *Solarcity Corp. v.*  
22 *Sunpower Corp.*, the plaintiff agreed that its declaratory relief claim overlapped with its other  
23 claims, and the Court was simply faced with the question whether to dismiss with or without  
24 prejudice. No. 16-CV-05509-LHK, 2017 WL 1739169, at \*3 (N.D. Cal. May 4, 2017). In *In re*  
25 *Zappos.com, Inc.*, the court concluded that a declaratory relief claim was “on its face duplicative”  
26 where it asked the court to declare that the defendant had violated the same state and federal laws  
27 already pled in the complaint. No. 12-CV-00325-RCJ, 2013 WL 4830497, at \*5 (D. Nev. Sept. 9,

2013). Here, the FAC provides a sufficient basis to conclude that the declaratory relief claim seeks something distinct from the contract claims.

Accordingly, the Court DENIES Defendant’s motion to dismiss Plaintiffs’ declaratory relief claim.

#### **E. CLRA**

In Count Eleven, Paid Users Plaintiff Mortensen asserts a claim against Yahoo under the CLRA, which prohibits “unfair methods of competition and unfair or deceptive acts or practices undertaken by any person in a transaction intended to result or that results in the sale or lease of goods or services to any consumer.” Cal. Civ. Code § 1770(a).

Defendants move to dismiss Paid User Plaintiff Mortensen’s CLRA claim on two grounds. First, Defendants argue that Plaintiff Mortensen does not sufficiently allege reliance as required for a CLRA claim. Mot. at 16. Second, Defendants argue that Yahoo’s email platform does not qualify as a “good” or “service” within the meaning of the CLRA. *Id.* The Court addresses each of these arguments in turn.

##### **1. Reliance**

Defendants first contend that Plaintiff Mortensen does not plead reliance. Mot. at 16. Specifically, Defendants fault Plaintiff Mortensen for failing to include any allegations that he “actually read” the alleged misrepresentations in the Terms of Service that give rise to Plaintiff Mortensen’s CLRA claim. *Id.* Plaintiffs counter that Plaintiff Mortensen’s claim is not premised on a misrepresentation in the Terms of Service but instead on Defendants’ material omissions about the security of their databases and the resulting breaches. Opp. at 17.

Defendants’ arguments fail for familiar reasons. Like with Plaintiffs’ deceit by concealment claim, Defendants point to a portion of this Court’s First MTD Order where the Court required Plaintiffs to plead that they actually read and relied on Defendants’ Privacy Policy. First MTD Order at 48–49. However, such an allegation was necessary in that situation because Plaintiffs’ theory depended on misrepresentations in the Privacy Policy. Here, in contrast, Plaintiff Mortensen’s theory is not that Yahoo made misrepresentations but instead that Yahoo

1 was obligated to disclose certain material facts. FAC ¶ 281. Plaintiff Mortensen alleges that  
 2 Yahoo had exclusive knowledge about the inadequacy of its security and contemporaneous  
 3 knowledge about the 2014 Breaches and Forged Cookie Breach but actively concealed those facts  
 4 from customers. *Id.* The FAC supports that, had Yahoo disclosed the breaches, the significant  
 5 media and expert attention would have alerted Plaintiff Mortensen and he would not have  
 6 provided his PII or signed up for Yahoo’s services. *Id.* ¶¶ 4, 132, 285. These allegations are  
 7 sufficient to conclude that if Yahoo had disclosed the security inadequacies and breaches, Plaintiff  
 8 Mortensen would have been aware and would have acted differently.

9 Defendants cannot overcome this conclusion by noting that they disclosed that Yahoo Mail  
 10 would not necessarily be secure because “no data transmission over the Internet or information  
 11 storage technology can be guaranteed to be 100% secure.” FAC, Ex. 13, at 1. Such a disclosure  
 12 does not undercut Plaintiffs’ contention that Yahoo had “exclusive knowledge of material facts not  
 13 known or reasonably accessible to” Plaintiffs. *Collins v. eMachines, Inc.*, 134 Cal. Rptr. 3d 588,  
 14 593 (Ct. App. 2011). Nor can Yahoo escape liability just because Plaintiff Mortensen does not  
 15 claim that he stopped using Yahoo Mail after learning of the breaches. *See* FAC ¶ 28. As  
 16 explained in the deceit by concealment section, Plaintiff Mortensen can simultaneously plead that  
 17 he took little action after learning of the security defects but that he would have acted differently if  
 18 he had been informed beforehand. *Id.* ¶ 285. Thus, Plaintiff Mortensen has adequately alleged  
 19 that he relied on Yahoo’s omissions. The Court next turns to Defendants’ broader argument that  
 20 the CLRA is inapplicable because Yahoo did not provide a “good” or “service.”

## 21 2. “Good” or “Service”

22 Defendants next contend that Yahoo Mail is neither a “good” nor a “service” and so does  
 23 not come within the ambit of the CLRA. Mot. at 16. The CLRA applies only to a limited set of  
 24 consumer transactions, and is not a law of “general applicability.” *Ting*, 319 F.3d at 1148. For  
 25 example, only a consumer may allege a violation of the CLRA. *See id.* A “consumer” is defined  
 26 as “an individual who seeks or acquires, by purchase or lease, any goods or services for personal,  
 27 family, or household purposes.” Cal. Civ. Code § 1761(d). “Goods” is defined as “tangible



1 chattels bought or leased for use primarily for personal, family, or household purposes.” *Id.*  
 2 § 1761(a). “Services” is defined as “work, labor, and services for other than a commercial or  
 3 business use.” *Id.* § 1761(b).

4 Defendants argue that software never qualifies as either a “good” or “service” under the  
 5 CLRA. Mot. at 16. For support, Defendants rely on two previous decisions by this Court—  
 6 *Ferrington v. McAfee*, No. 10-CV-01455-LHK, 2010 WL 3910169, at \*19 (N.D. Cal. Oct. 5,  
 7 2010), and *In re iPhone Application Litigation*, 844 F. Supp. 2d 1040, 1070 (N.D. Cal. 2012). The  
 8 holdings in those cases are not as expansive as Defendants suggest.

9 *Ferrington* involved computer software downloaded directly from the Internet. 2010 WL  
 10 3910169, at \*1. The Court did not hold that software can never constitute a “good,” but only “that  
 11 the software Plaintiffs purchased [was] not a good covered by the CLRA.” *Id.* at \*19 (emphasis  
 12 added). The Court based its analysis on the “CLRA’s express limitation of goods to ‘*tangible*  
 13 chattels.’” *Id.* (emphasis added). The Court’s statements do not foreclose the possibility that  
 14 software may sometimes qualify as a “good” under the CLRA. In fact, in *In re iPhone*, which was  
 15 decided shortly thereafter, this Court concluded that software downloaded into a tangible good  
 16 may be subject to the CLRA where the claim arises from the “sale of [the] good, and not the  
 17 downloading of free software.” 844 F. Supp. 2d at 1071; *see also In re Lenovo Adware Litig.*, No.  
 18 15-MD-02624-RMW, 2016 WL 6277245, at \*11 (N.D. Cal. Oct. 27, 2016) (denying motion to  
 19 dismiss because the “CLRA claim [was] premised on [the] purchase of Lenovo laptops,” not the  
 20 software installed on the laptop).

21 Certainly, too, software sold in a physical form may constitute “tangible chattels” and thus  
 22 qualify as a “good” under the CLRA because “[a] consumer can purchase [the software] in a store,  
 23 pick it up in her hands, and carry it home.” *Haskins v. Symantec Corp.*, No. 13-CV-01834-JST,  
 24 2013 WL 6234610, at \*9 (N.D. Cal. Dec. 2, 2013); *see also Ladore v. Sony Computer Entm’t Am.,*  
 25 *LLC*, 75 F. Supp. 3d 1065, 1073 (N.D. Cal. 2014) (noting that the plaintiff went to a physical store  
 26 location to purchase the tangible video game that came in a box with physical documents); *Perrine*  
 27 *v. Sega of Am., Inc.*, No. 13-CV-01962-JSW, 2013 WL 6328489, at \*4 (N.D. Cal. Oct. 3, 2013)

1 (determining that a video game purchased by plaintiffs qualified as a “good”).

2 As to whether the software at issue in *Ferrington* qualified as a “service,” this Court  
 3 merely stated one conclusory sentence with no analysis: “software generally is not a service for  
 4 purposes of the CLRA.” 2010 WL 3910169, at \*19. As that statement reflects, the Court did not  
 5 find that software never constitutes a “service” for purposes of the CLRA. Instead, a court must  
 6 analyze the particular facts at issue to determine whether the software at issue falls within the  
 7 definition of “service.” For example, Judge Tigar has explained that “there are good reasons to  
 8 consider antivirus software to be a ‘service’ under the CLRA, since it continually updates and runs  
 9 regular virus checking.” *Haskins*, 2013 WL 6234610, at \*9 n.9.

10 Here, Plaintiffs have adequately alleged that Defendants provide a “service” to Plaintiffs.  
 11 The FAC pleads that Yahoo Mail is “one of the oldest email services” and the “primary service”  
 12 provided by Yahoo. FAC ¶ 33. Unlike in *Ferrington*, Plaintiffs have not purchased software that  
 13 they downloaded from the Internet. Rather, Plaintiffs have signed up for accounts on a web-based  
 14 platform, maintained by Yahoo, where they can engage in activities ranging from private email  
 15 communication to bank and stock trading to photo storage. *Id.* That Yahoo continually upkeep  
 16 and updates the system further solidifies that Yahoo is providing a “service,” i.e., “work, labor,  
 17 and services for other than a commercial or business use.” Cal. Civ. Code § 1761(b). Moreover,  
 18 as noted above, the FAC’s repeated labeling of Yahoo’s offerings as “services” is supported by the  
 19 fact that Yahoo itself has Terms of *Service* and defines “Yahoo! *Services*” as including  
 20 “communications tools, forums, shopping *services*, search *services*, personalized content and  
 21 branded programming.” FAC ¶¶ 24–28, 30, 32, 173; Ex. 1, at 1 (emphases added). Thus,  
 22 Plaintiffs have adequately pled that Yahoo provides a “service” that is subject to the CLRA.

23 Accordingly, the Court DENIES Defendants’ motion to dismiss Plaintiff Mortensen’s  
 24 CLRA claim.

#### 25 **F. CRA**

26 In Counts Twelve and Thirteen, California Plaintiffs Heines and Dugas assert two claims  
 27 against Defendants under the CRA, Cal. Civ. Code § 1798.80 *et seq.*, on behalf of the putative

1 California subclass. The CRA “regulates businesses with regard to treatment and notification  
2 procedures relating to their customers’ personal information.” *Corona v. Sony Pictures Entm’t,*  
3 *Inc.*, No. 14-CV-09600-RGK, 2015 WL 3916744, at \*6 (C.D. Cal. June 15, 2015). Plaintiffs  
4 claim that Defendants violated §§ 1798.81.5 and 1798.82.

5 Defendants first contend that these claims should be dismissed as to the Forged Cookie  
6 Breach because neither Plaintiff Heines nor Plaintiff Dugas adequately alleges standing.

7 Defendants next make contentions specific to each of the two statutory sections.

8 The Court first analyzes Defendants’ standing argument, then analyzes the two statutory  
9 sections in turn.

### 10 **1. Standing**

11 Defendants move to dismiss Plaintiffs’ CRA claims to the extent they rely on the Forged  
12 Cookie Breach because, according to Defendants, Plaintiffs lack Article III standing to sue with  
13 respect to those claims. Article III standing to sue requires that (1) the plaintiff suffered an  
14 injury in fact, i.e., “an invasion of a legally protected interest which is (a) concrete and  
15 particularized, and (b) actual or imminent, not conjectural or hypothetical”; (2) the injury is  
16 “‘fairly traceable’ to the challenged conduct”; and (3) the injury is “likely” to be “redressed by a  
17 favorable decision.” *Lujan v. Def. of Wildlife*, 504 U.S. 555, 560–61 (1992). “The party invoking  
18 federal jurisdiction bears the burden of establishing these elements . . . with the manner and degree  
19 of evidence required at the successive stages of litigation.” *Id.* at 561. At the pleading stage,  
20 “[g]eneral allegations” of injury may suffice. *Id.*

21 Defendants contend that Plaintiffs lack Article III standing because Plaintiffs cannot  
22 establish “injury in fact.” Specifically, Defendants assert that Plaintiffs Heines and Dugas have  
23 not alleged any harm from the Forged Cookie Breach. Mot. at 17. Plaintiffs respond that  
24 Plaintiffs Heines and Dugas have plainly alleged injury from the Forged Cookie Breach. Opp. at  
25 24. Plaintiffs are correct.

26 Contrary to Defendants’ suggestion, the allegations for Plaintiffs Heines and Dugas are not  
27 limited to the 2013 Breach or the 2014 Breach. For example, Plaintiffs expressly allege that

United States District Court  
Northern District of California

1 “Plaintiffs Heines and Dugas . . . were deprived of prompt notice of the 2013, 2014, and Forged  
2 Cookie Breaches and were thus prevented from taking appropriate protective measures.” FAC  
3 ¶ 308. Likewise, Plaintiffs allege that Defendants’ failure to implement security measures resulted  
4 in the Forged Cookie Breach and that, “[a]s the direct and legal result . . . , Plaintiffs Heines and  
5 Dugas . . . were harmed because their PII and financial information were compromised.” *Id.*  
6 ¶ 295. Finally, both Plaintiff Heines and Plaintiff Dugas allege that they were affected by all of  
7 the breaches, though not singling out the Forged Cookie Breach specifically. *Id.* ¶¶ 18 (“[T]he  
8 Yahoo Data Breaches have caused Plaintiff Heines to be at substantial risk for further identity  
9 theft.”), 20 (“[T]he Yahoo Data Breaches have caused Plaintiff Dugas to be at substantial risk for  
10 further identity theft.”). Notwithstanding that the Forged Cookie Breach was a separate breach  
11 that affected a smaller number of users, *id.* ¶¶ 6, 117–18, the FAC alleges that Plaintiffs Heines  
12 and Dugas were among those affected.

13 Thus, Plaintiffs Heines and Dugas have adequately alleged that they suffered injury as a  
14 result of the Forged Cookie Breach. Having rejected Defendants’ standing argument as to both  
15 CRA statutory sections at issue, the Court next turns to each individual statutory section.

16 **2. Cal. Civ. Code § 1798.81.5 – Inadequate Security**

17 Plaintiffs assert that Defendants violated § 1798.81.5 of the CRA. This provision provides,  
18 in relevant part:

19 A business that owns, licenses, or maintains personal information about a  
20 California resident shall implement and maintain reasonable security procedures  
21 and practices appropriate to the nature of the information, to protect the personal  
22 information from unauthorized access, destruction, use, modification, or  
23 disclosure.

24 Cal. Civ. Code § 1798.81.5(b).

25 Defendants argue that CRA “reasonable security” measures were not required for  
26 California residents potentially affected by the 2013 and 2014 Breaches because, at the time of the  
27 2013 and 2014 Breaches, the CRA did not require Defendants to protect the personal information  
28 allegedly stolen. *See* Mot. at 25–26. Defendants’ argument requires understanding an amendment

1 to § 1798.81.5's definition of "personal information" that became effective on January 1, 2016.  
 2 Accordingly, the Court first addresses § 1798.81.5's definition of "personal information" and the  
 3 2016 amendment to that definition. The Court then addresses the parties' arguments regarding the  
 4 2013 and 2014 Breaches.

5 "Personal information" is defined in § 1798.81.5(d)(1) of the statute. In 2013 and 2014, at  
 6 the time of the 2013 and 2014 Breaches, the statute defined personal information as the following:

7 [A]n individual's first name or first initial and his or her last name in combination  
 8 with any one or more of the following data elements, when either the name or the  
 data elements are not encrypted or redacted:

9 (A) Social security number.

10 (B) Driver's license number or California identification card number.

11 (C) Account number, 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.

12 (D) Medical information.

13 Cal. Civ. Code § 1798.81.5(d)(1) (2014).

14 Significantly, the definition of "personal information" in the pre-2016 version of this  
 15 section of the CRA did not include "[a] username or email address in combination with a  
 16 password or security question and answer that would permit access to an online account." This  
 17 language was added to the definition of "personal information" in § 1798.81.5(d)(1) by an  
 18 amendment that became effective on January 1, 2016. The definition of personal information now  
 19 reads:

20 (A) An individual's first name or first initial and his or her last name in  
 21 combination with any one or more of the following data elements, when either the  
 name or the data elements are not encrypted or redacted:

22 (i) Social security number.

23 (ii) Driver's license number or California identification card number.

24 (iii) Account number, 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.

25 (iv) Medical information.

26 (v) Health insurance information.

27 (B) A username or email address in combination with a password or security  
 28 question and answer that would permit access to an online account.

Cal. Civ. Code § 1798.81.5(d)(1).

1 Defendants claim that the 2013 and 2014 Breaches revealed only online account  
2 information. Mot. at 26. Thus, Defendants argue, the 2013 and 2014 Breaches did not reveal  
3 “personal information” as that term was defined in the pre-2016 versions of the CRA, and so  
4 Defendants were not required to provide reasonable security measures at the time of the 2013 and  
5 2014 Breaches. *Id.* Defendants contend that, if the Court were to apply the 2016 amendment to  
6 Plaintiffs’ CRA claim regarding the 2013 and 2014 Breaches, the Court would be applying the  
7 amendments retroactively, which the Court may not do. *Id.* Plaintiffs do not engage with  
8 Defendants’ retroactivity argument because Plaintiffs argue that their claim is well-pled even  
9 under the pre-2016 version of the CRA. Opp. at 20–22.

10 Because Plaintiffs do not advocate for application of the 2016 version of the CRA, the  
11 Court conducts its analysis under the pre-2016 version. As noted above, the personal information  
12 protected by the pre-2016 version of the CRA includes an individual’s first name or initial and last  
13 name in combination with (1) a social security number, (2) a driver’s license or California ID card  
14 number, (3) an account number, credit or debit card number, in combination with a code or  
15 password that would provide access to a financial account, or (4) medical information. *See* Cal.  
16 Civ. Code § 1798.81.5(d)(1) (2014). The FAC alleges that “[d]uring the 2013 and 2014 Breaches,  
17 hackers were able to take the names, email addresses, telephone numbers, birth dates, passwords,  
18 and security questions of Yahoo account holders.” FAC ¶ 7. On its face, that information does  
19 not fit the pre-2016 definition of personal information. However, as a result of obtaining users’  
20 passwords and security questions, hackers were able to access “financial communications and  
21 records containing credit cards, retail accounts, banking, account passwords, IRS documents, and  
22 social security numbers from transactions conducted by email.” *Id.* Therefore, the question is  
23 whether Defendants are liable when hackers were able to retrieve personal information by logging  
24 into users’ accounts.

25 The Court concludes that Plaintiffs have not stated a claim on the facts of this case. The  
26 statute applies to “[a] business that owns, licenses, or maintains personal information” and  
27 imposes a duty to “protect the personal information from unauthorized access, destruction, use,

1 modification, or disclosure.” Cal. Civ. Code § 1798.81.5(b). Here, Plaintiffs do not argue that  
 2 Defendants “own, license, or maintain” the information in Plaintiffs’ emails. Rather, Defendants  
 3 require Plaintiffs to turn over their PII, which includes information such as name, email address,  
 4 birth date, gender, and ZIP code. FAC ¶¶ 37. In the 2013 and 2014 Breaches, the hackers  
 5 allegedly gained access to that information in addition to users’ passwords and security questions,  
 6 all of which Defendants had stored in their databases. *Id.* ¶¶ 7, 155. It is that information that  
 7 Defendants were required to protect from unauthorized access by adopting and maintaining  
 8 “reasonable security” measures.<sup>2</sup> Indeed, “the purpose of [the statute] is to encourage businesses  
 9 that own, license, or maintain personal information about Californians to provide reasonable  
 10 security for *that* information.” Cal. Civ. Code § 1798.81.5(a)(1) (emphasis added).

11 Accordingly, the Court GRANTS Defendants’ motion to dismiss the California Plaintiffs’  
 12 CRA § 1798.81.5 claim to the extent that claim is based on Defendants’ failure to provide  
 13 “reasonable security” measures as to the 2013 and 2014 Breaches. The Court dismisses with  
 14 prejudice because amendment appears futile, and Plaintiffs do not request an opportunity to  
 15 amend.

### 16 3. Cal. Civ. Code § 1798.82 – Delayed Notification

17 Plaintiffs also assert that Defendants violated § 1798.82 of the CRA. This provision  
 18 provides, in relevant part:

19 A person or business that conducts business in California, and that owns or  
 20 licenses computerized data that includes personal information, shall disclose a  
 21 breach of the security of the system following discovery or notification of the  
 22 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 . . . .

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

---

26  
 27 <sup>2</sup> The Court need not address whether a different result would obtain if hackers had gotten access  
 to email content by, for example, intercepting emails.

1 breach notification must take. *See id.* § 1798.82(d).

2 In the First MTD Order, this Court denied Defendant’s motion to dismiss Plaintiffs’ claim  
3 with respect to the 2014 Breach and the Forged Cookie Breach. First MTD Order at 92.  
4 However, this Court dismissed Plaintiffs’ claim with respect to the 2013 Breach because Plaintiffs  
5 did not include allegations about when Defendants “discover[ed]” or were “notif[ied]” of the 2013  
6 Breach. First MTD Order at 64; *see also id.* at 70 n.11 (noting that “Plaintiffs have not alleged  
7 when Defendants discovered the 2013 Breach”). Without such allegations, Plaintiffs had not  
8 adequately alleged that Defendants “unreasonably delay[ed]” in notifying Plaintiffs of the 2013  
9 Breach on December 14, 2016. *Id.* at 65. The Court granted leave to amend for Plaintiffs to  
10 “allege facts sufficient to show that Defendants unreasonably delayed in failing to notify Plaintiffs  
11 that the 2013 Breach occurred.” *Id.*

12 Defendants argue that Plaintiffs have failed to cure this deficiency. Specifically,  
13 Defendants contend that, in the FAC, “Plaintiffs provide no details regarding the actual discovery  
14 date of the 2013 Breach.” Mot. at 18. Plaintiffs admit that the FAC does not allege either an exact  
15 or approximate date that Defendants discovered the 2013 Breach, but argue that their allegations  
16 permit an inference that Defendants delayed anywhere from one to three years. Opp. at 22–23.  
17 Plaintiffs’ present allegations are insufficient.

18 As Plaintiffs concede, the FAC does not indicate, either explicitly or approximately, when  
19 Defendants discovered that the 2013 Breach had taken place. Plaintiffs ask the Court to make an  
20 inference that Defendants knew well before the December 2016 disclosure because Yahoo failed  
21 to fix any of the critical issues identified by the 2012 Mandiant report and the 2013 to 2016 Dell  
22 SecureWorks and Leaf SR security assessments. FAC ¶¶ 70–97. Such allegations may raise the  
23 prospect that Defendants should have *discovered* the 2013 Breach at an earlier date, but they do  
24 bear on when Defendants should have *notified* customers of the 2013 Breach because they say  
25 nothing about when Defendants actually discovered the 2013 Breach. Plaintiffs also point to their  
26 allegations that Defendants knew about the 2014 Breach and Forged Cookie Breach as they were  
27 happening but did not inform Plaintiffs of those breaches until September 2016 and February



1 2017, respectively. *Id.* ¶¶ 126, 142. Plaintiffs argue that “Defendants’ delays in notifying  
 2 consumers of the 2014 Breach and [the] Forged Cookie Breach support a finding that” Defendants  
 3 delayed in notifying consumers of the 2013 Breach. *Opp.* at 23. Such an inference is not  
 4 plausible when neither Plaintiffs nor the FAC offer any basis to compare the 2013 Breach to the  
 5 2014 Breach and the Forged Cookie Breach. Although the 2014 Breach and Forged Cookie  
 6 Breach are allegedly related, FAC ¶ 119, the 2013 Breach is not alleged to be related to either of  
 7 the previous breaches.

8 Plaintiffs’ allegations with respect to Yahoo’s October 2017 disclosure of the three billion  
 9 user account scope of the 2013 Breach further demonstrate the inadequacy of their pleadings on  
 10 this point. Plaintiffs allege that Yahoo announced in October 2017 that the 2013 Breach had  
 11 affected all three billion user accounts. *Id.* ¶ 145. Plaintiffs allege that Yahoo was first alerted to  
 12 the information that would lead to discovery of the full scope of the 2013 Breach by the end of  
 13 January 2017 but that Yahoo did not determine until months after the June 2017 acquisition by  
 14 Verizon that “closer to three billion, not one billion, accounts had been compromised in 2013.”  
 15 *Id.* ¶ 146. Again, Plaintiffs’ allegations are too uncertain to divine any date of discovery, whether  
 16 specific or estimated. Without more specific information, the Court cannot evaluate whether  
 17 Defendants unreasonably delayed in notifying customers about the extent of the 2013 Breach on  
 18 October 3, 2017.

19 In the First MTD Order, the Court noted that Plaintiffs failed to allege anything  
 20 “suggesting when Defendants learned of the 2013 breach.” First MTD Order at 65. Those  
 21 allegations were necessary to allow the Court to determine whether Defendants unreasonably  
 22 delayed in notifying Plaintiffs of the 2013 Breach (and, relatedly, which version of the CRA was  
 23 in effect). *Id.* at 64–65. Plaintiffs’ allegations remain insufficient. Thus, the Court GRANTS  
 24 Defendants’ motion to dismiss the California Plaintiffs’ CRA § 1798.82 claim to the extent that  
 25 claim is based on the 2013 Breach. The Court dismisses with prejudice because Plaintiffs have  
 26 failed to cure the deficiencies addressed in the First MTD Order.

### 27 **G. Punitive Damages**

1 Plaintiffs request that the Court award punitive damages in connection with their claims for  
2 deceit by concealment, negligence, breach of the implied covenant of good faith and fair dealing,  
3 misrepresentation, and violations of the CRA. FAC ¶¶ 211, 223, 255, 277, 297, 312. Defendants  
4 move to dismiss Plaintiffs' claims to the extent that they seek punitive damages. Mot. at 27.

5 As a preliminary matter, the parties disagree over the correct procedural mechanism to  
6 move for dismissal. Defendants bring their motion under Rule 12(b)(6) for failure to state a claim.  
7 Mot. at 28. Plaintiffs argue that use of Rule 12(b)(6) is improper in this scenario and that  
8 Defendants should have moved to strike under Rule 12(f). Opp. at 32 n.27. Rule 12(b)(6), not  
9 Rule 12(f), is the appropriate vehicle here.

10 Rule 12(f) permits a court to "strike from a pleading an insufficient defense or any  
11 redundant, immaterial, impertinent, or scandalous matter." Defendants' contention that Plaintiffs  
12 cannot seek punitive damages as a matter of law does not readily fit any of the grounds in Rule  
13 12(f). As the Ninth Circuit has held, "Rule 12(f) does not authorize district courts to strike claims  
14 for damages on the ground that such claims are precluded as a matter of law." *Whittlestone, Inc. v.*  
15 *Handi-Craft Co.*, 618 F.3d 970, 974–75 (9th Cir. 2010). Instead, "[t]he proper medium for  
16 challenging the sufficiency of factual allegations in a complaint is through Rule 12(b)(6) not Rule  
17 12(f)." *Consumer Sols. REO, LLC v. Hillery*, 658 F. Supp. 2d 1002, 1020 (N.D. Cal. 2009);  
18 *Parker v. Fid. Sec. Life Ins. Co.*, No. 06-CV-00654-AWI, 2006 WL 2190956, at \*5 (E.D. Cal.  
19 Aug. 1, 2006). Thus, the Court analyzes Defendants' motion regarding punitive damages pursuant  
20 to Rule 12(b)(6).

21 Defendants advance two arguments in support of dismissal of Plaintiffs' claims to the  
22 extent those claims seek punitive damages. First, Defendants argue that Plaintiffs have not alleged  
23 that an officer, director, or agent of Defendants committed an oppressive, fraudulent, or malicious  
24 act. Mot. at 28. Second, Defendants raise particular objections to certain of Plaintiffs' claims—  
25 namely, the claims for negligence, breach of the implied covenant of good faith and fair dealing,  
26 and violations of the CRA. *Id.* at 26–27. The Court first addresses Defendants' argument as to all  
27 claims, then addresses Defendants' argument as to individual claims.

1           **1. Acts by Agent, Officer, or Director**

2           Defendants first move to dismiss all of Plaintiffs’ claims to the extent those claims seek  
3           punitive damages on the ground that Plaintiffs have failed to allege that an officer, director, or  
4           agent committed the oppressive, fraudulent, or malicious acts. Mot. at 28. By statute, where a  
5           plaintiff proves “by clear and convincing evidence that the defendant has been guilty of  
6           oppression, fraud, or malice, the plaintiff, in addition to the actual damages, may recover  
7           [punitive] damages.” Cal. Civ. Code § 3294(a). Nevertheless, a corporate entity cannot commit  
8           willful and malicious conduct; instead, “the advance knowledge and conscious disregard,  
9           authorization, ratification or act of oppression, fraud, or malice must be on the part of an officer,  
10          director, or managing agent of the corporation.” *Id.* § 3294(b); *Taiwan Semiconductor Mfg. Co. v.*  
11          *Tela Innovations, Inc.*, No. 14-CV-00362-BLF, 2014 WL 3705350, at \*6 (N.D. Cal. July 24,  
12          2014) (“[A] company simply cannot commit willful and malicious conduct—only an individual  
13          can.”). Therefore, Plaintiffs must plead that an officer, director, or managing agent of Defendants  
14          committed an act of oppression, fraud, or malice.

15          Plaintiffs satisfy that standard by focusing on particular conduct by the CISOs. For  
16          example, then-CISO Justin Somani found “gaping holes in Yahoo’s data security” as early as  
17          2011, FAC ¶ 67, and also knew about the 2014 Breach as it was happening, *id.* ¶ 104, but took no  
18          specific action in response. When Bob Lord became CISO at Yahoo in October 2015, he  
19          identified the “security and endemic culture issues” as a problem. *Id.* ¶ 110. Moreover, although  
20          he was aware that a nation state actor may have been involved in the 2014 Breach and that the  
21          company’s response had been to “sweep it under the rug,” his approach was to continue to hide it  
22          from the public. *Id.* ¶¶ 111–12. Indeed, the FAC notes that Yahoo’s internal documents,  
23          including those between Bob Lord and Yahoo’s general counsel, “contradicted [Yahoo’s] public  
24          statements.” *Id.* ¶ 125. When Yahoo finally revealed in its 2016 10-K filing with the SEC that it  
25          had contemporaneous knowledge of the 2014 Breach, the 10-K filing failed to mention that both  
26          Bob Lord and Yahoo’s general counsel knew about the 2014 Breach. *Id.* ¶ 129. These  
27          circumstances make plausible Plaintiffs’ claim that high-ranking executives and managers at

1 Yahoo, including its CISO, committed oppressive, fraudulent, or malicious conduct.

2 Defendants read their cited authority too broadly. In *Xerox Corp. v. Far Western*  
3 *Graphics, Inc.*, the court found the pleadings defective because the plaintiff failed to “allege any  
4 conduct by an officer, director or managing agent of [the defendant] sufficient to support the  
5 imposition of punitive damages against [the defendant].” No. 03-CV-4059-JF, 2004 WL  
6 2271587, at \*2 (N.D. Cal. Oct. 6, 2004). Similarly, in *Taiwan Semiconductor*, the punitive  
7 damages allegations were insufficient because the plaintiff failed to “include the names or titles of  
8 any individual actor.” 2014 WL 3705350, at \*6. In contrast, Plaintiffs here include the names and  
9 titles of individual actors who are alleged to have committed malicious conduct supporting an  
10 award of punitive damages. Plaintiffs’ allegations are significantly more robust than those in  
11 *Taiwan Semiconductor* and *Far Western Graphics*. Plaintiffs have adequately pled that an officer,  
12 director, or managing agent of Defendants committed an act of oppression, fraud, or malice.

13 Because Defendants make no other punitive damages arguments with respect to the deceit  
14 by concealment and misrepresentation claims, the Court DENIES Defendants’ motion to dismiss  
15 Plaintiffs’ deceit by concealment and misrepresentation claims to the extent those claims seek  
16 punitive damages. Defendants make additional arguments for dismissal of the claims for  
17 negligence, breach of the implied covenant of good faith and fair dealing, and violations of the  
18 CRA to the extent those claims seek punitive damages. The Court therefore turns to these  
19 remaining arguments.

## 20 2. Individual Claims

21 Defendants next move to dismiss Plaintiffs’ claims for negligence, breach of the implied  
22 covenant of good faith and fair dealing, and violations of the CRA to the extent those claims seek  
23 punitive damages. Mot. at 26–27. The Court addresses these individual claims one at a time.

24 First, Defendants move to dismiss Plaintiffs’ claim for negligence. It is true that conduct  
25 which may be described as unreasonable or negligent generally “does not satisfy the highly  
26 culpable state of mind warranting punitive damages.” *Evans v. Home Depot U.S.A., Inc.*, No. 16-  
27 CV-07191-JSW, 2017 WL 679531, at \*2 (N.D. Cal. Feb. 21, 2017) (quoting *Woolstrum v.*

1 *Mailloux*, 190 Cal. Rptr. 729, 735 (App. Dep’t Super Ct. 1983)). Nevertheless, “even where the  
 2 claim formally sounds in negligence, if the plaintiff can make a showing that defendant’s conduct  
 3 goes beyond gross negligence and demonstrates a knowing and reckless disregard, punitive  
 4 damages *may* be available.” *Simplicity Int’l v. Genlabs Corp.*, No. 09-CV-06146-SVW, 2010 WL  
 5 11515296, at \*2 (C.D. Cal. Apr. 21, 2010) (citing *Sturges v. Charles L. Harney, Inc.*, 331 P.2d  
 6 1072, 1080 (Cal. Ct. App. 1958)). Here, Plaintiffs have alleged numerous fraudulent, malicious,  
 7 and oppressive acts on the part of Defendants, including that Defendants “did nothing to protect its  
 8 user data” and “made a conscious and deliberate decision not to alert any of Yahoo’s customers  
 9 that their PII had been stolen.” FAC ¶¶ 1, 9. Accordingly, the Court DENIES Defendants’ motion  
 10 to dismiss Plaintiffs’ negligence claim to the extent that claim seeks punitive damages.

11         Second, Defendants move to dismiss Plaintiffs’ claim for breach of the implied covenant  
 12 of good faith and fair dealing. Under California law, punitive damages are not available for  
 13 breach of contract claims. Cal. Civ. Code § 3294(a) (providing for punitive damages “[i]n an  
 14 action for the breach of an obligation not arising from contract”); *Applied Equip. Corp. v. Litton*  
 15 *Saudi Arabia Ltd.*, 869 P.2d 454, 460 (Cal. 1994). Thus, except in the insurance context, “an  
 16 award of punitive damages is not recoverable for breach of the implied covenant of good faith and  
 17 fair dealing.” *Monaco v. Bear Stearns Residential Mortg. Corp.*, 554 F. Supp. 2d 1034, 1043  
 18 (C.D. Cal. 2008); *see also Copesky v. Superior Court*, 280 Cal. Rptr. 338, 345 (Ct. App. 1991)  
 19 (“[T]here is only *one* category of business transactions which definitionally is amenable to tort  
 20 actions for contract breaches, and that is insurance.”). Plaintiffs cite no contrary authority.  
 21 Accordingly, the Court GRANTS Defendants’ motion to dismiss Plaintiffs’ claim for breach of  
 22 the implied covenant of good faith and fair dealing to the extent that claim seeks punitive  
 23 damages. Because Plaintiffs cannot pursue punitive damages for this claim as a matter of law, the  
 24 Court grants dismissal with prejudice.

25         Third, and finally, Defendants move to dismiss the California Plaintiffs’ claims under the  
 26 CRA. “[W]here a statute *creates* new rights and obligations not previously existing in the  
 27 common law, the express statutory remedy is deemed to be the exclusive remedy available for  
 28

United States District Court  
Northern District of California

1 statutory violations, unless it is inadequate.” *Brewer v. Premier Golf Props.*, 86 Cal. Rptr. 3d 225,  
 2 232 (Ct. App. 2008) (quoting *De Anza Santa Cruz Mobile Estates Homeowners Ass’n v. De Anza*  
 3 *Santa Cruz Mobile Estates*, 114 Cal. Rptr. 2d 708, 725 (Ct. App. 2001)). The CRA, which  
 4 governs the “treatment and notification procedures relating to . . . customers’ personal  
 5 information,” *Corona*, 2015 WL 3916744, at \*6, was passed in 2000 and is not asserted to have  
 6 any common-law analogue. Additionally, the CRA contains a provision spelling out the damages  
 7 that a plaintiff may recover. *See* Cal. Civ. Code § 1798.84. While the CRA allows for civil  
 8 penalties when a defendant willfully, intentionally, or recklessly violates a section not at issue  
 9 here, *see id.* § 1798.84(c), the CRA does not allow for such penalties based on violations of the  
 10 statutes at issue here or expressly allow for punitive damages. Plaintiffs make no argument  
 11 otherwise. Accordingly, the Court GRANTS Defendants’ motion to dismiss the California  
 12 Plaintiffs’ CRA claims to the extent those claims seeks punitive damages. Because Plaintiffs  
 13 cannot pursue punitive damages for these claims as a matter of law, the Court grants dismissal  
 14 with prejudice.

15 **V. CONCLUSION**

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

- 18 • The Court GRANTS WITH PREJUDICE Defendants’ motion to dismiss the UCL  
 19 unlawful and unfair claims of Plaintiffs Rivlin and Granot, but DENIES  
 20 Defendants’ motion to dismiss the UCL unlawful and unfair claims of Plaintiff  
 21 Mortensen. In the First MTD Order, the Court denied Defendants’ motion to  
 22 dismiss the UCL unlawful and unfair claims of all other Plaintiffs.
- 23 • The Court DENIES Defendants’ motion to dismiss Plaintiffs’ deceit by  
 24 concealment claim.
- 25 • The Court DENIES Defendants’ motion to dismiss Plaintiffs’ negligence claim.
- 26 • The Court DENIES Defendants’ motion to dismiss Plaintiffs’ claim for breach of  
 27 contract.

28

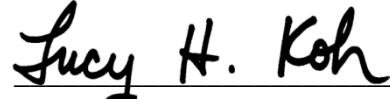
1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

- The Court DENIES Defendants’ motion to dismiss Plaintiffs’ claim for breach of implied contract.
- The Court GRANTS WITH PREJUDICE Defendants’ motion to dismiss Plaintiffs’ claim for breach of the implied covenant of good faith and fair dealing to the extent that claim seeks punitive damages, but otherwise DENIES Defendants’ motion to dismiss Plaintiffs’ claim for breach of the implied covenant of good faith and fair dealing.
- The Court DENIES Defendants’ motion to dismiss Plaintiffs’ declaratory relief claim.
- In the First MTD Order, the Court denied Defendants’ motion to dismiss the fraudulent prong of Small Business Users Plaintiff Neff’s UCL claim.
- The Court DENIES Defendants’ motion to dismiss Small Business Users Plaintiff Neff’s misrepresentation claim to the extent that claim seeks punitive damages.
- The Court DENIES Defendants’ motion to dismiss Plaintiff Mortensen’s CLRA claim.
- The Court GRANTS WITH PREJUDICE Defendants’ motion to dismiss the California Plaintiffs’ CRA § 1798.81.5 claim to the extent that claim is based on the 2013 and 2014 Breaches. The Court also GRANTS WITH PREJUDICE Defendants’ motion to dismiss the California Plaintiffs’ CRA § 1792.81.5 claim to the extent that claim seeks punitive damages.
- The Court GRANTS WITH PREJUDICE Defendants’ motion to dismiss the California Plaintiffs’ CRA § 1798.82 claim to the extent that claim is based on the 2013 Breach. In the First MTD Order, the Court denied Defendants’ motion to dismiss the California Plaintiffs’ CRA § 1798.82 claim to the extent that claim is based on the 2014 Breach or the Forged Cookie Breach. The Court also GRANTS WITH PREJUDICE Defendants’ motion to dismiss the California Plaintiffs’ CRA § 1798.82 claim to the extent that claim seeks punitive damages.

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

**IT IS SO ORDERED.**

Dated: March 9, 2018



---

LUCY H. KOH  
United States District Judge

United States District Court  
Northern District of California