

**MORGAN & MORGAN  
COMPLEX LITIGATION GROUP**  
John A. Yanchunis (Admitted Pro Hac Vice)  
201 N. Franklin Street, 7th Floor  
Tampa, Florida 33602  
Telephone: 813/223-5505  
813/223-5402 (fax)  
*jyanchunis@ForThePeople.com*

**CASEY GERRY SCHENK  
FRANCAVILLA BLATT & PENFIELD  
LLP**  
Gayle M. Blatt, SBN 122048  
110 Laurel Street  
San Diego, CA 92101  
Telephone: 619/238-1811  
619/544-9232 (fax)  
*gmb@cglaw.com*

**MILBERG LLP**  
Ariana J. Tadler (Admitted Pro Hac Vice)  
One Pennsylvania Plaza  
New York, NY 10119  
Telephone: 212/594-5300  
212/868-1229 (fax)  
*atadler@milberg.com*

**ROBBINS GELLER RUDMAN  
& DOWD LLP**  
Stuart A. Davidson (Admitted Pro Hac Vice)  
120 East Palmetto Park Road, Suite 500  
Boca Raton, FL 33432  
Telephone: 561/750-3000  
561/750-3364 (fax)  
*sdavidson@rgrdlaw.com*

**LOCKRIDGE GRINDAL NAUEN P.L.L.P.**  
Karen Hanson Riebel (Admitted Pro Hac Vice)  
100 Washington Ave. South, Suite 2200  
Minneapolis, MN 55401  
Telephone: 612/339-6900  
612/339-0981 (fax)  
*khriebel@locklaw.com*

*Attorneys for Plaintiffs and the Class*

**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA  
SAN JOSE DIVISION**

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

CASE NO. 16-MD-02752-LHK

**CONSOLIDATED CLASS ACTION  
COMPLAINT**

JURY TRIAL DEMANDED

1 Plaintiffs Kimberly Heines, Hashmatullah Essar, Paul Dugas, Matthew Ridolfo, Deana  
 2 Ridolfo, Rajesh Garg, Scarleth Robles, Maria Corso, Jose Abitbol, Yaniv Rivlin, and Mali Granot,  
 3 by and through undersigned counsel, on behalf of themselves and all others similarly situated, allege  
 4 the following claims and causes of action against Defendant Yahoo! Inc. (“Yahoo”), and Plaintiff  
 5 Brian Neff, on behalf of himself and all others similarly situated, alleges the following claims and  
 6 causes of action against Defendants Yahoo and Aabaco Small Business, LLC (“Aabaco”)  
 7 (collectively with Yahoo, “Defendants”), based upon personal knowledge as to Plaintiffs and  
 8 Plaintiffs’ own acts, and on information and belief as to all other matters based upon, *inter alia*, the  
 9 investigation conducted by and through Plaintiffs’ counsel as follows:

### 10 **SUMMARY OF THE CASE**

11 1. In September 2016, Yahoo rocked the technology world by disclosing that  
 12 information was stolen from 500 million user accounts two years earlier in the then-largest known  
 13 data breach in history (the “2014 Breach”). Only two months later, Yahoo again made headlines  
 14 when it admitted to an even more massive breach—affecting upwards of 1 billion user accounts—  
 15 that had occurred *three years* before Yahoo made the admission (the “2013 Breach”). During both of  
 16 these breaches, hackers stole the names, email addresses, telephone numbers, birth dates, passwords,  
 17 and security questions of Yahoo account holders. They also gained access to the email contents of all  
 18 breached Yahoo accounts and thus any private information contained within those emails, such as  
 19 financial communications and records involving credit cards, retail accounts, banking, account  
 20 passwords, IRS documents, and social security numbers from transactions conducted by email, in  
 21 addition to other confidential and sensitive information contained therein. This compromised data is  
 22 collectively referred to as “Personal Identifying Information” or “PII.”

23 2. Recently, after the anticipated sale of Yahoo to Verizon was renegotiated to shave  
 24 \$350 million off of the purchase price, Yahoo began notifying approximately 32 million Yahoo  
 25  
 26  
 27  
 28

1 users that they had been the victim of yet another breach; this time a “forged cookie” data breach in  
2 2015-2016 (the “Forged Cookie Breach”).<sup>1</sup>

3 3. Despite the staggering magnitude of these breaches, Yahoo claimed it did not  
4 discover the 2014 Breach or 2013 Breach until 2016. However, Yahoo’s internal documents clearly  
5 show this is false. In fact, Yahoo knew about the 2014 Breach *at the time it was occurring*.

6 4. In its most recent 10-K filing with the SEC, Yahoo admitted an independent  
7 investigation showed it had “contemporaneous knowledge” of the 2014 Breach, yet failed to  
8 “properly investigate[] and analyze[]” the breach, due in part to “failures in communication,  
9 management, inquiry and internal reporting” that led to a “lack of proper comprehension and  
10 handling” of the 2014 Breach.”<sup>2</sup> The 10-K provided additional details regarding Yahoo’s failures:

11 Specifically, as of December 2014, the information security team  
12 understood that the attacker had exfiltrated copies of user database backup  
13 files containing the personal data of Yahoo users but it is unclear whether  
14 and to what extent such evidence of exfiltration was effectively  
15 communicated and understood outside the information security team.  
16 However, the Independent Committee did not conclude that there was an  
17 intentional suppression of relevant information.

18 Nonetheless, the Committee found that the relevant legal team had  
19 sufficient information to warrant substantial further inquiry in 2014, and  
20 they did not sufficiently pursue it. As a result, the 2014 Security Incident  
21 was not properly investigated and analyzed at the time, and the Company  
22 was not adequately advised with respect to the legal and business risks  
23 associated with the 2014 Security Incident. The Independent Committee  
24 found that failures in communication, management, inquiry and internal  
25 reporting contributed to the lack of proper comprehension and handling of  
26 the 2014 Security Incident. The Independent Committee also found that  
27 the Audit and Finance Committee and the full Board were not adequately  
28 informed of the full severity, risks, and potential impacts of the 2014  
Security Incident and related matters.<sup>3</sup>

---

25 <sup>1</sup> The 2013 Breach, 2014 Breach, and Forged Cookie Breach are collectively referred to as the  
26 “Yahoo Data Breaches.”

27 <sup>2</sup> Yahoo!, Inc. 2016 Form 10-K (March 1, 2017), at 47, [https://investor.yahoo.net/secfiling.cfm?](https://investor.yahoo.net/secfiling.cfm?filingID=1193125-17-65791&CIK=1011006)  
filingID=1193125-17-65791&CIK=1011006.

28 <sup>3</sup> *Id.*

1           5.       Even more astoundingly, Yahoo did not own up to the 2013 Breach—the one  
2 involving 1 billion accounts—until three years after it happened. At the time of the 2013 Breach,  
3 Yahoo was still using an encryption technology called MD5, which at least five years earlier had  
4 been both publicly discredited and deemed “cryptographically broken and unsuitable for further  
5 use.”<sup>4</sup> So, identity thieves had three full years of unfettered access to the inadequately-encrypted PII  
6 of roughly 1 billion user accounts before Yahoo even notified its users that their PII had been  
7 compromised.

8           6.       Both the scope of these three massive data breaches and Yahoo’s baffling and  
9 unlawful delay in notification is unprecedented in the information technology world. Yahoo stands  
10 alone as the world’s worst offender when it comes to protecting its users’ privacy.

11          7.       This Consolidated Class Action Complaint is filed on behalf of all persons, described  
12 more fully in the following sections, whose PII was compromised in the 2103, 2014, or Forged  
13 Cookie Data Breaches. The class representatives here have all suffered actual harm, including but  
14 not limited to having false tax returns filed in their name, having credit card accounts fraudulently  
15 opened in their names, having fraudulent charges posted to their credit cards and bank accounts,  
16 having their government benefits stolen, and having spam and phishing emails sent constantly from  
17 their Yahoo address. The compromise of the Class members’ PII has also caused the Class members  
18 to pay for credit monitoring, account freezes, card and account replacements, and late fees for  
19 delayed payments. Class members have devoted and will continue to devote time and energy into  
20 recovering stolen funds (where possible), tracking and repairing damage to their credit reports and  
21 reputations, and monitoring and protecting their accounts. Plaintiffs and Class members are further  
22 damaged as their PII remains in Defendants’ possession, without adequate protection, and is also in  
23 the hands of those who obtained it for its commercial value, without Plaintiffs’ or Class members’  
24 consent.

25  
26  
27 <sup>4</sup> Joseph Menn, Jim Finkle, & Dustin Volz, INSIGHT-Yahoo security problems a story of too little,  
28 too late, CNBC (Dec. 18, 2016, 5:09 PM), <http://www.cnbc.com/2016/12/18/reuters-america-insight-yahoo-security-problems-a-story-of-too-little-too-late.html>.

## **JURISDICTION AND VENUE**

8. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act (“CAFA”), 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds \$5,000,000, exclusive of interests and costs, there are more than 100 class members, and at least one class member is a citizen of a state different from Defendants and is a citizen of a foreign state. Subject matter jurisdiction also arises under 28 U.S.C. § 1331 based on the claim asserted under the Federal Stored Communications Act, 18 U.S.C. § 2702. The Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

9. Venue is proper under 28 U.S.C. § 1391(c) because Defendants are corporations that do business in and are subject to personal jurisdiction in this District. Venue is also proper under 28 U.S.C. § 1391(b) based on the Transfer Order of the Judicial Panel on Multidistrict Litigation, Dkt. No. 62, and because a substantial part of the events or omissions giving rise to the claims in this action occurred in or emanated from this District, including the decisions made by Yahoo’s governance and management personnel that led to the breaches. Further, Yahoo’s and Aabaco’s terms of service governing users in the United States and Israel provide for California venue for all claims arising out of Plaintiffs’ relationship with Yahoo and/or Aabaco.

## **PARTIES**

### **A. Class Representatives Who Signed up for Yahoo Services in the United States**

10. Plaintiff Kimberly Heines is a resident and citizen of Magalia, California. Ms. Heines receives approximately \$1,100 per month from Social Security Disability to meet her essential needs, including food and housing. Plaintiff Heines opened a Yahoo account nearly twenty years ago and used it for all of her online communication, including communications relating to her education, financial aid, employment, banking, healthcare, and personal finances. The PII Plaintiff Heines had occasion to include in Yahoo emails included information relating to her account with Direct Express, the payment service through which she receives her Social Security Disability benefits. On February 4, 2015, Plaintiff Heines discovered that her entire monthly disability allowance had been stolen from her Direct Express account and used to purchase gift cards at Rite Aid (in the amounts of \$513.58 and \$507.10), and Walgreens, (in the amount of \$118.00). Plaintiff Heines had her Direct

1 Express card in her possession at the time of the thefts, and was away from home caring for a  
2 hospitalized relative, more than 600 miles from where the thefts occurred. Because she had no other  
3 source of income, the theft put her in an extremely vulnerable and stressful situation in which she  
4 literally had to rely on the kindness of strangers to survive for two weeks. Plaintiff Heines is  
5 normally very conscientious about paying bills on time but the theft caused her to pay her rent and  
6 some utility bills late, which resulted in late fees of more than \$30. Soon after the theft, Ms. Heines  
7 started receiving collection calls regarding debts she had not incurred. She also saw unfamiliar debts  
8 appearing on her credit report and her credit score suffered as a result. Plaintiff Heines filed a police  
9 report and spent over 40 hours talking to the police, the Social Security Administration, Direct  
10 Express, RiteAid, Walgreens and others to have the funds restored to her Direct Express account and  
11 deal with other consequences of the data breach, the resulting theft, and the consequences of the  
12 theft. In or about September 2016, Plaintiff Heines received an email notice from Yahoo informing  
13 her that her Yahoo accounts and PII may have been compromised in the 2014 Breach.

14 11. Plaintiff Hashmatullah Essar is a resident and citizen of Thornton, Colorado. Mr.  
15 Essar is a retail manager for a local bank and handles retail and banking accounts. Approximately 15  
16 years ago, Mr. Essar opened two email accounts with Yahoo. Mr. Essar used his Yahoo email  
17 accounts for all of his personal, financial, and business needs. More specifically, Plaintiff Essar  
18 transacted business, shopped online, sent personal messages, communicated with his accountant,  
19 received bank account statements, applied for jobs, secured a mortgage for his home, and refinanced  
20 that mortgage, through his Yahoo e-mail account. Plaintiff Essar first became concerned about the  
21 security of his Yahoo email accounts when he received phishing emails from a credit card company  
22 purporting to be affiliated with American Express, asking him to follow a link to log-in to his  
23 “Serve” account. Plaintiff Essar knew the email to be false because he did not have a “Serve”  
24 account through American Express. Subsequently, in October 2016, Mr. Essar received an email  
25 notice from Yahoo notifying him of the 2014 Breach, and informing him that his Yahoo accounts  
26 and PII may have been compromised. As a result of the breach notification, and concerned for his  
27 own and his family’s well-being, Plaintiff Essar signed up for a credit counseling class through his  
28 employer to learn how to limit, recognize, and respond to identity theft. In addition, as a direct result

1 of the 2014 Breach, Mr. Essar signed up for and paid (and continues to pay) \$35.98 per month for  
2 LifeLock credit monitoring service. Notwithstanding his attempts to limit the damage done to his  
3 credit and identity as a result of the 2014 Breach, Mr. Essar has suffered great harm as a result of the  
4 Breach. Plaintiff Essar not only lost years of email messages when several hundred simply vanished  
5 from his Yahoo account, he also experienced tax fraud in February 2017, when an unauthorized  
6 person fraudulently filed a tax return under his Social Security Number. Further, Mr. Essar was  
7 denied credit in March 2017 due to the identity theft he suffered as a result of the 2014 Breach, and  
8 freezes were placed on his credit. Finally, because Plaintiff Essar is a United States citizen of  
9 Afghani descent, he worries that a terrorist sympathizer may steal his PII and may use it to commit  
10 crimes in his name, so much so that he suffers from extreme anxiety and has difficulty sleeping.

11 12. Plaintiff Paul Dugas is a resident and citizen of San Diego, California. Plaintiff Dugas  
12 is a semi-retired real estate investor and banker. Mr. Dugas has opened four Yahoo accounts over  
13 approximately the last twenty years. He used his Yahoo accounts for his banking, investment  
14 accounts, business emails, and personal emails. Plaintiff Dugas's 2013 and 2014 business tax returns  
15 were compromised, and he is still attempting to resolve the matter. As a result, his business has had  
16 to pay penalties and otherwise been financially penalized. In April of 2016, Plaintiff Dugas was  
17 unable to file his personal tax return because the Internal Revenue Service stated that a tax return  
18 had already been filed under his Social Security Number. As a result of his inability to file a tax  
19 return in 2016, both of his college-aged daughters missed deadlines to submit the Free Application  
20 for Federal Student Aid (FAFSA). Because Plaintiff Dugas' daughters were unable to file for  
21 FAFSA, he paid \$5,000 tuition for one daughter and \$4,000 room and board for the other—expenses  
22 that he would not have had to cover had his daughters been able to file for FAFSA, as they had in the  
23 past. Plaintiff Dugas also experienced numerous fraudulent charges on his personal and business  
24 Bank of America and Navy Federal Credit Union credit cards. He has had to replace his Bank of  
25 America credit card numerous times and his Navy Federal credit card replaced once Plaintiff Dugas  
26 has paid \$30.00 to three different credit bureaus to freeze his accounts. Finally, Plaintiff Dugas paid  
27 extra fees and costs to his Certified Public Accountant to help sort out the tax return problems  
28 suffered as a result of the Breach.



1           13.     Plaintiffs Matthew and Deana Ridolfo are a married couple and residents and citizens  
2 of Vineland, New Jersey. Plaintiff Deanna Ridolfo works with a public school system and Plaintiff  
3 Matthew Ridolfo is a mechanical designer for a local company. Both Plaintiffs used their Yahoo  
4 accounts for nearly twenty years, for general banking, credit card management and communications,  
5 a mortgage refinance, and communication with friends and family. In June 2016, Plaintiff Matthew  
6 Ridolfo used his Yahoo email account to send scanned copies of sensitive financial documents in  
7 order to refinance the couple's home mortgage. Shortly thereafter, in December 2016, both Mr. and  
8 Mrs. Ridolfo received notice of the 2013 Breach. On January 4, 2017, Plaintiff Deana Ridolfo  
9 received a letter from Citibank informing her that Citibank was concerned that her Citibank card was  
10 fraudulently accessed. Since Plaintiff Deana Ridolfo had never opened a Citibank account, she  
11 immediately knew it was a fraudulent card. Mrs. Ridolfo contacted Citibank immediately and  
12 learned that cash advances and Uber charges were listed on the account that had been opened in her  
13 name. Citibank also informed her that a second Citibank account was recently applied for in her  
14 name, this one for a Sears branded credit card. As a result of the letter and information received from  
15 Citibank, the Ridolfos immediately obtained free credit reports through Experian. Plaintiff Deana  
16 Ridolfo learned that someone attempted to open an account at Barclay Bank, two accounts at Lowes,  
17 and a Walmart account in her name. Further, Mrs. Ridolfo learned that an American Express account  
18 was fraudulently opened in her name, and \$900.00 had been charged on a fraudulently opened  
19 Target credit card. Mr. Ridolfo learned that a total of eleven credit card or bank accounts had been  
20 fraudulently opened or attempted to be opened during the month of December 2016 in his name  
21 through the following retailers and banks: Brooks Brothers, Brandsource, Citi Doublecash, Capital  
22 One, Walmart, Lowes, Sears Mastercard, TD Bank, Barclays Bank of Delaware, Santander Bank,  
23 and Banco Popular of Puerto Rico. In addition, fraudulent addresses were listed for the Ridolfos in  
24 Florida and Virginia. As a result of this significant fraud, both Plaintiffs Matthew and Deana Ridolfo  
25 were forced to individually call each bank to report the fraudulent accounts and charges, spending  
26 significant time talking with credit card fraud departments. Further, unauthorized persons hacked  
27 into their personal home phone line through Comcast, forwarded their home line phone calls to an  
28 unknown phone number, and ordered additional phone lines under their names. Plaintiffs Matthew



1 and Deana Ridolfo made countless phone calls to credit card companies, Experian, TransUnion,  
2 Equifax, Innovis, the Internal Revenue Department, the Department of Motor Vehicles, and the  
3 Social Security Administration to help protect their sensitive and confidential information. Further,  
4 the Ridolfos were forced to file police reports in New Jersey, Florida and Virginia to protect their  
5 identity. Finally, Plaintiffs Matthew and Deana Ridolfo purchased and enrolled in LifeLock to have  
6 help monitoring their credit and finances, expending approximately \$30.00 per month each for a  
7 total of over \$60.00 per month. Despite enrolling in a credit monitoring program, placing freezes on  
8 their credit, and individually notifying credit card companies and banks, an unauthorized person  
9 opened another credit card account on January 31, 2017 in Plaintiff Deana Ridolfo's name.

10 14. Plaintiff Rajesh Garg is a resident and citizen of Naperville, Illinois. Plaintiff Garg is  
11 a software testing engineer and has worked in that industry for over ten years. Plaintiff Garg opened  
12 a Yahoo email account nearly twenty years ago. Plaintiff Garg is a small business owner and used  
13 his Yahoo email account to make software and electronics purchases for his small business. Plaintiff  
14 Garg maintained over 500 business and personal contacts through his Yahoo email account. In  
15 addition, Plaintiff Garg used his Yahoo account for banking, investment accounts, business emails,  
16 banking, credit card, healthcare, social security, and for friends and family. Plaintiff Garg also used  
17 Yahoo Flickr to store and maintain hundreds of personal videos and photos of his children, including  
18 from when they were young. Plaintiff Garg began noticing large amounts of emails with  
19 pornographic pictures being sent to his Yahoo email address. Plaintiff Garg then learned that his  
20 Yahoo account had been breached when an unauthorized person(s) sent emails on his behalf to his  
21 personal and professional contacts about "the usefulness of Viagra," "the benefits of a Russian  
22 bride," and "sex toys." As a result of the Yahoo breach, Plaintiff Garg sent individual apology letters  
23 to professional and personal contacts due to the embarrassing emails fraudulently sent on his behalf.  
24 Further, Plaintiff Garg feared the exposure of his children from the hundreds of photos stored in  
25 Yahoo Flickr. In or about the last quarter of 2016, Plaintiff Garg received notice from defendant  
26 Yahoo that his PII had been compromised due to a data breach.

**B. Class Representatives for the Israel Class**

15. Plaintiff Yaniv Rivlin is a resident of Tel Aviv, Israel, and has dual Israeli and Canadian citizenship. Plaintiff Rivlin opened his Yahoo email account in Israel approximately ten years ago mainly for personal purposes, including banking, friends and family, credit card statements, and social security administration. Plaintiff Rivlin pays Yahoo annually \$20.00 to have Yahoo emails received forwarded to another email account. Plaintiff Rivlin maintains a credit card on file with Yahoo to pay for the forwarding service. Plaintiff Rivlin was notified on December 20, 2016 from Yahoo that his Yahoo email account had been breached. After the notification, Plaintiff Rivlin noticed an increase in unsolicited emails, including spam and advertisements. Plaintiff Rivlin also spent, and continues to spend, considerable time and effort proactively changing username and passwords on many of his accounts to prevent fraud.

16. Plaintiff Mali Granot is a resident and citizen of Raanana, Israel. Plaintiff Granot maintained a Yahoo email account, which she opened in Israel, for personal reasons, specifically to correspond with family, friends and school. Plaintiff Granot was unexpectedly locked out of her Yahoo email account and unable to gain access. Plaintiff Granot eventually gained access to her Yahoo email account by answering security questions. However, once she opened her Yahoo email account, she received unsolicited pop-up chat requests and other unsolicited requests including for services that she had not requested but that someone had requested in her name using her Yahoo email account.

**C. Class Representative for the Venezuela Class**

17. Plaintiff Scarleth Robles is a resident and citizen of Venezuela. Plaintiff Robles opened and maintained a Yahoo email account beginning in 2013 through a Venezuela Yahoo server and sent her PII to Yahoo to be securely stored. Plaintiff Robles uses her Yahoo email account primarily for professional correspondence. In particular, Ms. Robles advises entrepreneurs on business ventures and ideas and requests that potential clients send their entrepreneurial and business proposals to her Yahoo email address. Plaintiff Robles discovered that an unknown person(s) accessed her Yahoo email account in or around September 2016 and stole business ideas from her email account. Plaintiff Robles also witnessed business proposals in her Yahoo email inbox but then

1 they immediately disappeared and she was unable to contract with potential business partners as a  
 2 direct result. As a result of the Yahoo Data Breaches, Plaintiff Robles lost approximately ten clients  
 3 for her professional business. The Yahoo Data Breaches compromised her credibility and the  
 4 security of her small business, in addition to causing her PII to be at substantial risk for identity theft,  
 5 if it has not already been stolen.

6 **D. Class Representatives for the Australia and Spain Class**

7 18. Plaintiff Maria Corso is a resident and citizen of Clearview, South Australia. Plaintiff  
 8 Corso signed up for Yahoo services in Australia. Plaintiff Corso maintained two Yahoo email  
 9 accounts, both of which she used to send sensitive information, including financial documents, her  
 10 tax security number, work history, and medical information. Plaintiff Corso ceased using one of her  
 11 Yahoo email accounts in June 2016. In early September 2016, Plaintiff Corso was locked out of her  
 12 remaining Yahoo email account without warning. Two days later, Plaintiff Corso saw television  
 13 reports of the 2014 Breach. Plaintiff Corso immediately contacted who she believed to be Yahoo  
 14 customer service and was advised that Russian state actors had accessed her Yahoo email account.  
 15 Yahoo customer service also confirmed to Plaintiff Corso that Russian hackers tried over 60 times to  
 16 gain access to her Yahoo email account. As a direct result of the 2014 Breach, on September 26,  
 17 2016, Plaintiff Corso purchased account security protection from a company she believed was  
 18 affiliated with Yahoo. Plaintiff Corso understood that she was required to purchase account security  
 19 protection in order to regain access to her Yahoo account and to secure her private information in her  
 20 breached email account. Plaintiff Corso continues to pay an annual fee in the amount of \$150.00  
 21 U.S. dollars for the security protection offered by a company she believes to be affiliated with  
 22 Yahoo. Plaintiff Corso has spent countless hours contacting Yahoo to secure her information in her  
 23 email account. Despite her efforts, Plaintiff Corso still receives “failed attempt” messages from  
 24 Yahoo as a result of unauthorized person(s) attempting to gain access to her Yahoo email account.

25 19. Plaintiff Jose Abitbol is a resident of New York but a citizen of Spain. Plaintiff  
 26 Abitbol signed up for a Yahoo email account, and maintains his account, through the Spanish Yahoo  
 27 host. Plaintiff Abitbol uses his email account to transact personal and professional business. Plaintiff  
 28 Abitbol’s Yahoo email account contains sensitive and confidential information, including

1 information about his bank accounts, business, investment accounts, credit cards, personal matters,  
 2 and social security number. Plaintiff Abitbol received two notices from Yahoo, one notifying him  
 3 that his email account was breached in 2013 and the second notifying him that his email account was  
 4 breached in 2016. In September 2016, an unknown person(s) accessed Plaintiff Abitbol's Yahoo  
 5 email account and sent emails on his behalf to his bank in Israel requesting a wire transfer totaling  
 6 \$30,000 U.S. dollars. Plaintiff Abitbol's bank, unaware of the breach, complied with the instructions  
 7 from the fraudulent email request and wire transferred \$30,000 U.S. dollars to an account held by the  
 8 fraudulent requestor(s). Plaintiff Abitbol did not know at the time that his Yahoo email had been  
 9 breached or that an unknown person requested wire transfers but noticed the missing money. When  
 10 Plaintiff Abitbol used his Yahoo email account to contact the bank to inquire about the funds  
 11 transfer, the unknown fraudulent person(s) intercepted his emails and responded on behalf of the  
 12 bank. Plaintiff Abitbol became suspicious of the content of the bank email messages and contacted  
 13 the bank. Plaintiff Abitbol was eventually reimbursed for the illegally transferred \$30,000, but only  
 14 after he spent hours resolving the problem. The fraudulent person(s) obtained Plaintiff Abitbol's  
 15 bank account number through his Yahoo email account. This time, the fraudulent requestor sent an  
 16 email, again impersonating Mr. Abitbol through his Yahoo email account, to Plaintiff Abitbol's  
 17 business partner requesting \$20,000 U.S. dollars emergency use. It is currently unknown how many  
 18 other times these unknown person(s) impersonated Plaintiff Abitbol to illegally obtain money or  
 19 information.

20 **E. Class Representatives for the Small Business Users Class**

21 20. Plaintiff Brian Neff is a citizen and resident of Texas. In September 2009, in  
 22 connection with his online insurance agency business, he contracted with Yahoo for two services,  
 23 Yahoo! Web Hosting for www.TheInsuranceSuite.com and Yahoo! Business Email, for which he  
 24 has paid Yahoo \$13.94 every month through the date of this Complaint. Between 2009 and the  
 25 present, at various times, Mr. Neff has used Defendants' web hosting services in connection with  
 26 another 54 websites, paying anywhere from \$3.94 to \$15.94 per month for each website. On  
 27 December 14, 2016, Plaintiff Neff received a notice from Yahoo informing him that hackers had  
 28 stolen account information that he had provided to Defendants—information that “may have

1 included names, email addresses, telephone numbers, dates of birth, hashed passwords (using  
2 outdated encryption) and, in some cases, encrypted or unencrypted security questions and answers.”  
3 In addition to paying Yahoo thousands of dollars for services that subjected him to security breaches,  
4 Plaintiff Neff was also a victim of actual identity theft which, upon information and belief, was  
5 caused by one or more of the Yahoo Data Breaches. In May 2015, he incurred fraudulent charges on  
6 his Capital One credit card and his Chase debit card, both of which were on file with Yahoo to pay  
7 for services connected with two of his websites, with Yahoo being the only company to which  
8 Plaintiff Neff had provided information about both accounts. In addition to these fraudulent charges,  
9 also in May 2015, an unauthorized credit card account in Plaintiff Neff’s name was opened at Credit  
10 One Bank, and unauthorized and fraudulent charges were made to that account in May and June  
11 2015. Plaintiff Neff had to spend significant time and incurred expenses mitigating the harm to him  
12 from these security breaches and identity theft. As to both the Capital One and Chase cards, Plaintiff  
13 Neff had to make several phone calls to each to notify them of the fraudulent charges and to have the  
14 accounts frozen. He had to change passwords for both cards and he then had to wait two to four days  
15 to receive new cards from each. As to the Credit One Bank credit card opened in his name, Plaintiff  
16 Neff had to call the police department and file a police report, fill out an FTC affidavit, engage in  
17 multiple phone calls to Credit One over several weeks totaling multiple hours, and put together a  
18 package of materials for Credit One, which took hours, and which was sent to Credit One via  
19 Federal Express overnight delivery at a cost of \$11.87. In addition, at a time when Plaintiff Neff was  
20 trying to pre-qualify for a home mortgage, he learned that his credit reports contained negative  
21 information about overlimits and unpaid charges on the fraudulent Credit One Bank credit card. He  
22 had to write a demand letter to Credit One Bank to force it to contact Experian and TransUnion and  
23 have these negative items removed from his credit reports. Since these incidents, Plaintiff Neff has  
24 been reviewing reports from complimentary credit monitoring offered by all his credit cards which  
25 offer that complimentary service, reviewing daily updates from Credit Karma, and has ordered and  
26 reviewed free annual reports from all three credit bureaus—all activities to which he has been  
27 required to devote many hours of time. Now that he is aware of the inadequacy of Defendants’  
28 online security, Plaintiff Neff has stopped using the site, costing him many valuable leads for

insurance business. Further, Plaintiff Neff intends to migrate his insurance agency website, www.TheInsuranceSuite.com, to a more secure provider. The cost to transfer Plaintiff Neff's accounts and services currently with Defendants to a company with adequate security is in excess of \$10,000, due to the nature and capacity of his website, and the cost to reestablish the high search engine placement he has earned over the last eight years, among other factors.

## **F. Defendants**

21. Yahoo is a Delaware corporation registered with the California Secretary of State, with its principal place of business and headquarters in Sunnyvale, California, located at 701 First Ave., Sunnyvale, CA 94089.

22. Aabaco is a wholly owned and controlled subsidiary of Yahoo. Its headquarters and principal place of business are the same as Yahoo's headquarters in Sunnyvale, California. Since November 2015, Aabaco has been the business entity that Yahoo uses to provide services to small business owners. Before that date, Yahoo provided the same services through one of its divisions, Yahoo Small Business. After the transition to Aabaco, Yahoo reassured its subscribers that the change was in name only, greeting them with the following account sign-in notice: "Yahoo Small Business is now Aabaco Small Business. Same Team. Same Passion to grow your business. Different name."

23. At all times herein relevant, Aabaco has been the alter ego of Yahoo for its small business subscribers, and has been wholly owned and managed by Yahoo. Yahoo and Aabaco are also joint venturers and are jointly responsible to small business customers for any wrongful acts carried out by Aabaco that are material to this suit. Finally, Aabaco is the successor in interest to the Yahoo Small Business division and is liable to small business customers, in addition to Yahoo, as the successor for any wrongdoing by that division before it was dissolved by Yahoo and re-named Aabaco.

## **FACTUAL BACKGROUND**

### **A. Yahoo Collects and Stores PII for its Own Financial Gain**

24. One of the web's earliest pioneers, Yahoo was founded in 1994 as a directory of websites, but quickly developed into a source for searches, email, shopping, and news. Currently, its

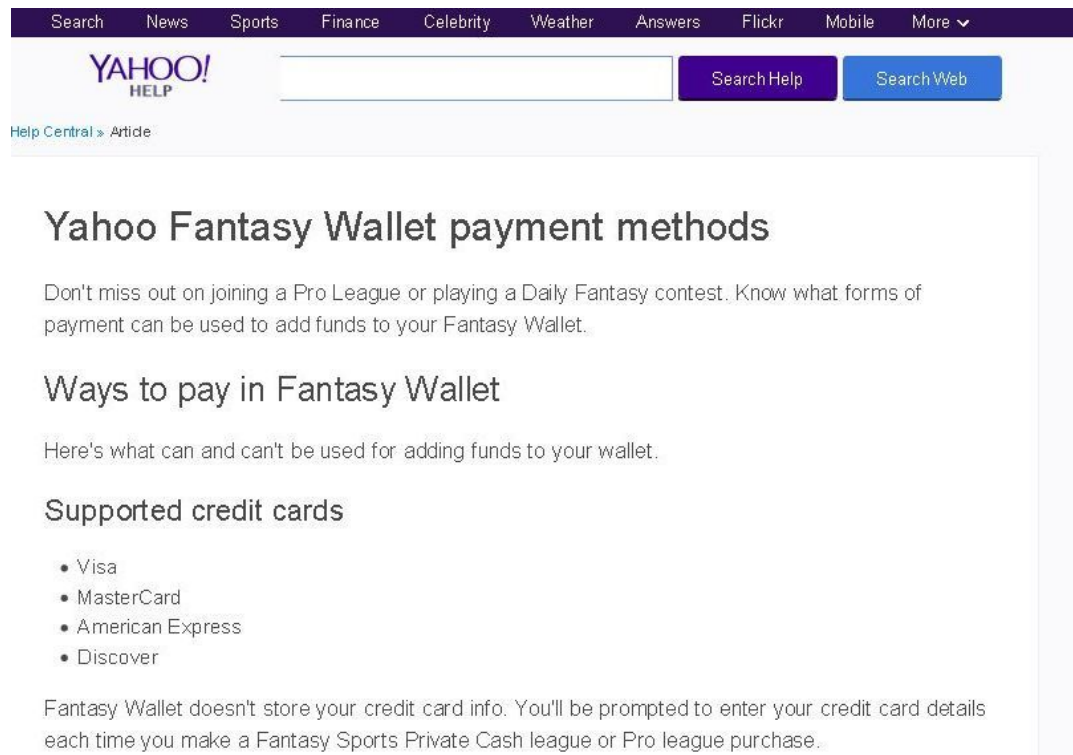
services attract at least one billion visitors per month. Yahoo sister sites include Flickr, Yahoo Finance, and Yahoo Fantasy Sports, among others.

25. Yahoo's primary service across all its offerings is Yahoo Mail, one of the oldest free email services. Many users have built their digital identities around Yahoo Mail, using the service for everything from their bank and stock trading accounts to photo albums and even medical information. Moreover, users not only use their Yahoo Mail accounts for private email communications, but they also use them as recovery and log-in credentialing points for accounts on many other websites. Yahoo allows anyone who is over the age of 12 to open a Yahoo account.

26. Yahoo also offers a variety of other services, including Yahoo Messenger (an instant messaging service), news, financial, and sports sites, and a social networking site called Tumblr.

27. Yahoo also offers online services that require entry of credit card and other financial information, such as the popular Yahoo Fantasy Sports leagues.

28. The Yahoo Fantasy Sports leagues use what Yahoo calls "Yahoo Wallet," in which users can enter a variety of credit card, debit card, and other account information.<sup>5</sup>



<sup>5</sup> Yahoo Fantasy Wallet payment methods, Yahoo! Help, <https://help.yahoo.com/kb/SLN26520.html> (last visited Apr. 8, 2017).



29. Yahoo also offers various online services to small businesses. Popular services include website hosting, which makes it easy for businesses to create and operate a business website, advertising for those businesses, and email services for communications between businesses and their customers. To obtain these services, small businesses or their owners have to set up accounts with Yahoo and/or Aabaco and provide credit card or debit card information for automatic monthly payments. Yahoo originally provided these services through a division called Yahoo Small Business. Since November 2015, Yahoo has provided its small business services through its wholly owned subsidiary Aabaco.

30. When users establish any of the above account accounts with Defendants, users must provide Defendants with PII, which, upon information and belief, Defendants then electronically collect, store on, and route through its U.S.-based servers, a majority of which are located in California. And, in fact, Plaintiffs and Class members signed up for online Yahoo accounts and provided the required PII, including, in some cases, debit and credit card information, which, Defendants collected, stored, and routed through its U.S.-based servers.

31. Plaintiffs and Class members signed up for online Yahoo accounts that required them to provide many different sorts of personal information, including, in some cases, debit and credit card information.

32. The “Privacy Center” portion of Yahoo’s website explains the type of personal information it collects directly from its account holders:<sup>6</sup>

#### **Information Collection & Use**

##### **General**

Yahoo collects personal information when you register with Yahoo, when you use Yahoo products or services, when you visit Yahoo pages or the pages of certain Yahoo partners, and when you enter promotions or sweepstakes. Yahoo may combine information about you that we have with information we obtain from business partners or other companies.

When you register we ask for information such as your name, email address, birth date, gender, ZIP code, occupation, industry, and personal interests. For some financial products and services we might also ask for your address, Social Security number, and information about your assets. When you register with Yahoo and sign in to our services, you are not anonymous to us.

Yahoo collects information about your transactions with us and with some of our business partners, including information about your use of financial products and services that we offer.

<sup>6</sup> Yahoo Privacy Center, Yahoo!, <https://policies.yahoo.com/us/en/yahoo/privacy/index.htm> (last visited Apr. 5, 2017).

33. Yahoo also informs its account holders that it shares personal information provided by account registrants only under limited circumstances:<sup>7</sup>

### Information Sharing & Disclosure

Yahoo does not rent, sell, or share personal information about you with other people or non-affiliated companies except to provide products or services you've requested, when we have your permission, or under the following circumstances:

- We provide the information to trusted partners who work on behalf of or with Yahoo under confidentiality agreements. These companies may use your personal information to help Yahoo communicate with you about offers from Yahoo and our marketing partners. However, these companies do not have any independent right to share this information.
- We have a parent's permission to share the information if the user is a child under age 13. See [Children's Privacy & Family Accounts](#) for more information about our privacy practices for children under 13.
- We respond to subpoenas, court orders, or legal process (such as [law enforcement requests](#)), or to establish or exercise our legal rights or defend against legal claims.
- We believe it is necessary to share information in order to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of Yahoo's terms of use, or as otherwise required by law.
- We transfer information about you if Yahoo is acquired by or merged with another company. In this event, Yahoo will notify you before information about you is transferred and becomes subject to a different privacy policy.

Yahoo displays targeted advertisements based on personal information. Advertisers (including ad serving companies) may assume that people who interact with, view, or click targeted ads meet the targeting criteria—for example, women

34. Yahoo represented and warranted to Plaintiffs and the Class members that its PII databases were secure and that customers' PII would remain private. In particular, Yahoo represented that **“protecting our systems and our users' information is paramount to ensuring Yahoo users enjoy a secure user experience and maintaining our users' trust.”**<sup>8</sup> Yahoo further assured users that “[w]e have physical, electronic, and procedural safeguards that comply with federal regulations to protect personal information about you.”<sup>9</sup>

35. Defendants made similar representations about the importance of security on Aabaco's website: “We have physical, electronic, and procedural safeguards that comply with federal regulations to protect your Personal Information.”<sup>10</sup>

<sup>7</sup> *Id.*

<sup>8</sup> [Security at Yahoo](https://policies.yahoo.com/us/en/yahoo/privacy/topics/security/index.htm), Yahoo!, <https://policies.yahoo.com/us/en/yahoo/privacy/topics/security/index.htm> (last visited Apr. 8, 2017).

<sup>9</sup> *Id.*

<sup>10</sup> [Privacy Policy](https://www.aabacosmallbusiness.com/privacy-policy), Yahoo! Aabaco Small Business, <https://www.aabacosmallbusiness.com/privacy-policy> (last visited Apr 9, 2017).

36. Defendants thus collect and store tremendous amounts of PII, and use this information to maximize profits through targeted advertising and other means. Defendants also assure that they take user privacy and safeguarding of PII very seriously. The facts show otherwise.

**B. PII is Very Valuable on the Black Market**

37. The types of information compromised in the Yahoo Data Breaches are highly valuable to identity thieves. In addition to credit and debit card information, names, email addresses, recovery email accounts, telephone numbers, dates of birth, passwords and security question answers can all be used to gain access to a variety of existing accounts and websites. Indeed, Plaintiffs and Class members have suffered a variety of consequences from the breach, including forged credit applications, the opening of unauthorized credit card accounts, fake IRS tax returns being filed under the user's name, fraudulent charges, email hacks, unauthorized access to payment accounts such as PayPal and Western Union, stolen gift card account numbers redeemable at online merchants, and numerous other identity theft-related damages.

38. Identity thieves can also use the PII to harm Plaintiffs and Class members through embarrassment, blackmail or harassment in person or online, or to commit other types of fraud including obtaining ID cards or driver's licenses, fraudulently obtaining tax returns and refunds, and obtaining government benefits. A Presidential Report on identity theft from 2008 states that:

In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.

In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for

future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.<sup>11</sup>

39. To put it into context, as demonstrated in the chart below, the 2013 Norton Report, based on one of the largest consumer cybercrime studies ever conducted, estimated that the global price tag of cybercrime was around \$113 billion at that time, with the average cost per victim being \$298 dollars. That number will no doubt increase exponentially after the massive Yahoo Data Breaches.



40. The problems associated with identity theft are exacerbated by the fact that many identity thieves will wait years before attempting to use the PII they have obtained. Indeed, a Government Accountability Office study found that “stolen data may be held for up to a year or more before being used to commit identity theft.”<sup>12</sup> In order to protect themselves, class members will need to remain vigilant against unauthorized data use for years and decades to come.

41. Once stolen, PII can be used in a number of different ways. One of the most common is that it is offered for sale on the “dark web,” a heavily encrypted part of the Internet that makes it difficult for authorities to detect the location or owners of a website. The dark web is not indexed by normal search engines such as Google and is only accessible using a Tor browser (or similar tool), which aims to conceal users’ identities and online activity. The dark web is notorious for hosting

<sup>11</sup> The President’s Identity Theft Task Force, Combating Identity Theft: A Strategic Plan, Federal Trade Commission, 11 (April 2007), <http://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf>.

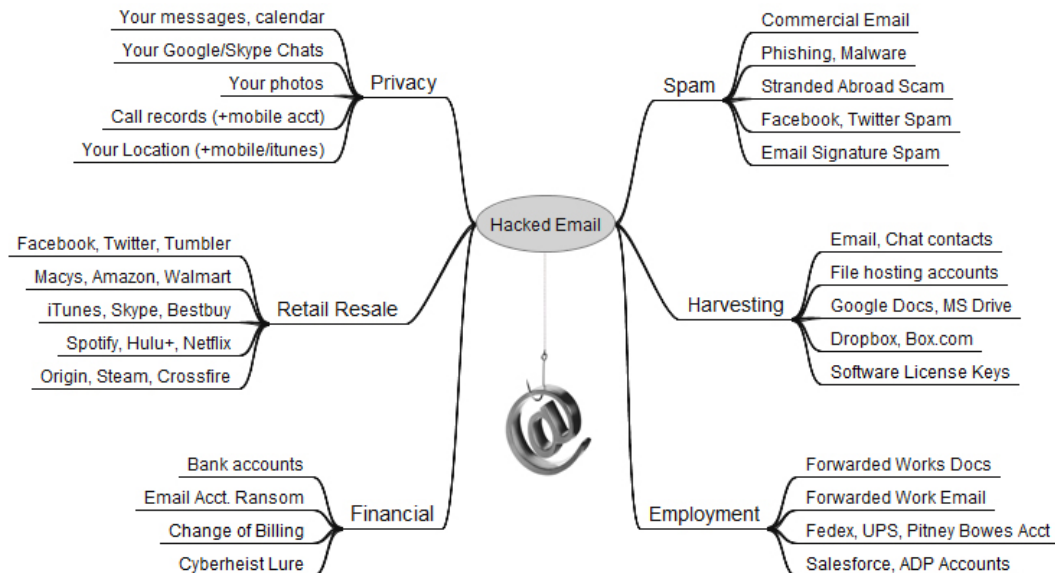
<sup>12</sup> Report to Congressional Requesters, U.S. Government Accountability Office, 33 (June 2007), available at [www.gao.gov/new.items/d07737.pdf](http://www.gao.gov/new.items/d07737.pdf).

marketplaces selling illegal items such as weapons, drugs, and PII.<sup>13</sup> Websites appear and disappear quickly, making it a very dynamic environment.

42. Once someone buys PII, it is then used to gain access to different areas of the victim's digital life, including bank accounts, social media, and credit card details. During that process, other sensitive data may be harvested from the victim's accounts, as well as from those belonging to family, friends, and colleagues.

43. In addition to PII, a hacked email account can be very valuable to cyber criminals. Since most online accounts require an email address not only as a username, but also as a way to verify accounts and reset passwords, a hacked email account could open up a number of other accounts to an attacker.<sup>14</sup>

44. As shown in the chart below, a hacked email account can be used to link to many other sources of information for an identity thief, including any purchase or account information found in the hacked email account:<sup>15</sup>



<sup>13</sup> Brian Hamrick, The dark web: A trip into the underbelly of the internet, WLWT News (Feb. 9, 2017 8:51 PM), <http://www.wlwt.com/article/the-dark-web-a-trip-into-the-underbelly-of-the-internet/8698419>.

<sup>14</sup> Identity Theft and the Value of Your Personal Data, Trend Micro (Apr. 30, 2015), <https://www.trendmicro.com/vinfo/us/security/news/online-privacy/identity-theft-and-the-value-of-your-personal-data>.

<sup>15</sup> Brian Krebs, The Value of a Hacked Email Account, KrebsOnSecurity (June 13, 2013, 3:14 PM), <https://krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account/>.



**C. Yahoo Fails to Upgrade Its Security After Repeated Intrusions**

45. Yahoo has a storied, unfortunate history with hacking. Since at least 2001, Yahoo has been repeatedly put on notice that its security measures were not up to par, leaving users' PII at risk of theft. Rather than addressing the problems by upgrading its data security, Yahoo continued to use outdated security methods long after vulnerabilities were brought to Yahoo's attention.

46. In 2001, then-20-year-old hacker Adrian Lamo showed he could rewrite published articles on Yahoo! News without even having to enter a password.<sup>16</sup>

47. In 2012, Yahoo admitted that more than 450,000 user accounts were compromised through an SQL injection attack—with the passwords simply stored in plain text. This breach revealed that Yahoo apparently had failed to take even basic precautions to protect its customers' data. Indeed, news outlets reported that “[s]ecurity experts were befuddled ... as to why a company as large as Yahoo would fail to cryptographically store the passwords in its database. Instead, they were left in plain text, which means a hacker could easily read them.”<sup>17</sup>

48. According to Marcus Carey, a security researcher at Rapid7, the 2012 hack showed Yahoo was far behind the times. “It is definitely poor security. It’s not even security 101. It’s basic application development 101.”<sup>18</sup> Indeed, the Federal Trade Commission considered SQL injection attacks a known—and preventable—threat as far back as 2003.<sup>19</sup>

49. The 2012 hack was meant – and should have served – as a “wake up call” to Yahoo that its protections for users' personal information were inadequate. In fact, on the webpage where the information from that hack was dumped, there was a message purportedly from the hackers that read:

---

<sup>16</sup> Kevin Poulsen, Yahoo! News Hacked, SecurityFocus (Sept. 18, 2001), <http://www.securityfocus.com/news/254>.

<sup>17</sup> Antone Gonsalves, Yahoo security breach shocks experts, CSO (July 12, 2012, 8:00 AM), <http://www.csoonline.com/article/2131970/identity-theft-prevention/yahoo-security-breach-shocks-experts.html>.

<sup>18</sup> *Id.*

<sup>19</sup> In the Matter of Guess?, Inc., and Guess.com, Inc., FTC Matter No. 022 3260, 3 (Jul. 30, 2003), available at <https://www.ftc.gov/sites/default/files/documents/cases/2003/08/guesscomp.pdf>.

We hope that the parties responsible for managing the security of this subdomain will take this as a wake-up call, and not as a threat ... There have been many security holes exploited in Web servers belonging to Yahoo! Inc. that have caused far greater damage than our disclosure. Please do not take them lightly.<sup>20</sup>

50. Unfortunately, Yahoo's internal culture actively discouraged emphasis on data security. For example, former Yahoo security staffers interviewed later told Reuters that requests made by Yahoo's security team for new tools and features such as strengthened cryptography protections were, at times, rejected on the grounds that the requests would cost too much money, were too complicated, or were simply too low a priority.<sup>21</sup>

51. To make matters worse, Yahoo has experienced other security breaches since the 2013 Breach occurred but before either the 2013 Breach or 2014 Breach was made public in 2016. For example, in late December 2013, hackers found an exploit targeting Java in Yahoo's ad network, which affected primarily users in Europe and was infecting roughly 27,000 computers *per hour* at the time of discovery.<sup>22</sup>

52. None of these intrusions prompted Yahoo to comprehensively review and ameliorate its shoddy security, allowing the 2014 Breach and the Forged Cookie Breach to occur.

#### **D. Yahoo's Inadequate Data Security Allows the Massive Breach of 1 Billion User Accounts in 2013, Which Yahoo Then Fails to Disclose**

53. As an example of Yahoo's refusal to keep abreast of cybersecurity issues, in the summer of 2013, Yahoo decided to finally abandon the use of a discredited technology for encrypting data known as MD5. While this may seem like a forward-thinking move, MD5 was well known as a weak password protection method by hackers and security experts for years before the

---

<sup>20</sup> Doug Gross, Yahoo hacked, 450,000 passwords posted online, CNN (July 13, 2012, 9:31 AM), <http://www.cnn.com/2012/07/12/tech/web/yahoo-users-hacked/>.

<sup>21</sup> Reuters, Why Yahoo's Security Problems Are a Story of Too Little, Too Late, FORTUNE (Dec. 18, 2016), <http://fortune.com/2016/12/19/yahoo-hack-cyber-security/>.

<sup>22</sup> Andrew Scurria, European Yahoo Users Victimized In Malware Attack, Law360 (Jan. 6, 2014, 6:02 PM), <https://www.law360.com/articles/498914/>.



2013 Breach. MD5 can be cracked more easily than other so-called “hashing” algorithms, which are mathematical functions that convert data into seemingly random character strings.<sup>23</sup>

54. In fact, five years before Yahoo finally took action, Carnegie Mellon University’s Software Engineering Institute issued a public warning to security professionals through a U.S. government-funded vulnerability alert system, stating that: MD5 “should be considered cryptographically broken and **unsuitable for further use.**”<sup>24</sup>

55. “MD5 was considered dead long before 2013,” said David Kennedy, chief executive of cyber firm TrustedSec. “Most companies were using more secure hashing algorithms by then.”<sup>25</sup> Common techniques such as “salting” (adding a unique secret to the password) and “stretching” (repeating the hashing process over many times) hashed passwords makes them far harder for hackers to decode.<sup>26</sup> Stronger hashing technology would have made it more difficult for the hackers to get into customer accounts after breaching Yahoo’s network, making the attack far less damaging, according to five former employees and some outside security experts.<sup>27</sup> But with MD5, there are vast indexes of these pre-computed MD5 hashes—known as “rainbow tables”—freely available online that can be used to quickly crack a large percentage of any MD5 password list.<sup>28</sup>

56. Thus, when Yahoo finally began to upgrade from MD5 in the summer of 2013, it was too late. In August 2013, hackers breached more than one billion Yahoo accounts, stealing the poorly encrypted passwords and other information in the biggest data breach on record to date.

---

<sup>23</sup> Reuters, Why Yahoo’s Security Problems Are a Story of Too Little, Too Late, FORTUNE (Dec. 18, 2016), <http://fortune.com/2016/12/19/yahoo-hack-cyber-security/>.

<sup>24</sup> Vulnerability Note VU#836068, Vulnerability Notes Database (Last revised Jan. 21, 2009), <https://www.kb.cert.org/vuls/id/836068>.

<sup>25</sup> Reuters, *supra* note 23.

<sup>26</sup> Mark Stockley, Yahoo breach: I’ve closed my account because it used MD5 to hash my password, naked security (Dec. 15, 2016), <https://nakedsecurity.sophos.com/2016/12/15/yahoo-breach-ive-closed-my-account-because-it-uses-md5-to-hash-my-password/>; Adam Bard, 3 Wrong Ways to Store a Password, adambard.com (July 11, 2013), <https://adambard.com/blog/3-wrong-ways-to-store-a-password/>.

<sup>27</sup> Stockley, *supra* note 26; Bard, *supra* note 26.

<sup>28</sup> Brian Krebs, My Yahoo Account Was Hacked! Now What?, KrebsOnSecurity (Dec. 15, 2016), <https://krebsonsecurity.com/2016/12/my-yahoo-account-was-hacked-now-what/>.

1           57.     Yahoo’s failure to move away from MD5 in a timely fashion was indicative of  
2 systemic problems in Yahoo’s security operations. One cybersecurity expert said, “even by 2013  
3 anyone with half a clue in securing passwords already long ago knew that storing passwords in MD5  
4 format was no longer acceptable and altogether braindead idea. It’s one of many reasons I’ve  
5 encouraged my friends and family to ditch Yahoo email for years.”<sup>29</sup>

6           58.     In the 2013 Breach, hackers obtained, among other things, class members’ Yahoo  
7 login (ID), Country Code, Recovery E-Mail (linked with the profile), Date of Birth (DOB), Hash of  
8 Password (MD5), and Cell phone number and ZIP code if they were provided by the user for  
9 password recovery.<sup>30</sup> Although Yahoo asserts that the Breaches did not expose credit card data (and  
10 there is little reason at this point to credit that claim), the Breaches allowed criminals to obtain  
11 passwords and login information for Yahoo users’ email accounts and, thus, obtain the actual content  
12 of users’ emails. Consequently, any sensitive data or documents contained in those emails could be  
13 compromised—not just credit card numbers, but bank account numbers, Social Security numbers,  
14 driver’s license numbers, passport information, birth certificates, deeds, mortgages, and contracts, to  
15 name just a few examples.

16           59.     One analyst, Jeff Williams, CTO of Contrast Security, characterized the 2013 Breach  
17 as “the Exxon Valdez of security breaches” given the fact that “1 billion accounts [were]  
18 compromised, when there are only 3 billion people with Internet access in the world.”<sup>31</sup>

19           60.     Tyler Moffitt, senior threat research analyst at Webroot, said: “All of the data stolen,  
20 including emails, passwords and security questions, make a potent package for identify theft. The  
21 main email account has links to other online logins and the average user likely has password overlap  
22 with multiple accounts.”<sup>32</sup>

23 \_\_\_\_\_  
24 <sup>29</sup> *Id.*

25 <sup>30</sup> InfoArmor: Yahoo Data Breach Investigation, InfoArmor (Sept. 28, 2016),  
<https://www.infoarmor.com/infoarmor-yahoo-data-breach-investigation/>.

26 <sup>31</sup> James Rogers, Yahoo hack: The 'Exxon Valdez of security breaches', Fox News (Dec. 15, 2016),  
<http://www.foxnews.com/tech/2016/12/15/yahoo-hack-exxon-valdez-security-breaches.html>.

27 <sup>32</sup> Samuel Gibbs, Security experts: 'No one should have faith in Yahoo at this point', the guardian  
28 (Dec. 15, 2016, 7:29 AM), <https://www.theguardian.com/technology/2016/dec/15/security-experts->

61. Moffitt takes little comfort from Yahoo's belated efforts to secure user accounts, stating, "These accounts have been compromised for years and the sheer number of them means they have already been a large source of identity theft. No one should have faith in Yahoo at this point."<sup>33</sup>

**E. Yahoo's Security Is Breached Again in 2014, 2015, and 2016—Yet Yahoo Still Does Not Alert Its Users**

62. In late 2014, hackers again accessed Yahoo accounts and this time stole information from at least 500 million user accounts. Yahoo knew about the 2014 Breach while it was happening, and even gave it an internal code name: the "Siberian Intrusion." Still, Yahoo took no further action, including failing to notify its users of the Breach.<sup>34</sup>

63. There are significant overlaps between the 2013 Breach and the 2014 Breach. In a February 23, 2017 letter to John Thune, Senate Chairman of the Committee on Commerce, Science and Transportation and Jerry Moran, Senate Chairman of the Subcommittee on Consumer Protection, Product Safety, Insurance and Data Security, Yahoo advised that it believes "[a] majority of the user accounts that were potentially affected by the 2014 Incident are also believed to have been affected by the 2013 Incident."<sup>35</sup>

64. Matt Blaze, a cyber security expert and director of the Distributed Systems Lab at the University of Pennsylvania likened the 2014 Breach to an "ecological disaster."



matt blaze @mattblaze · Sep 22

Password (& security Q) reuse means that data breaches on the scale of Yahoo are the security equivalent of ecological disasters.



106



97



yahoo-hack.

<sup>33</sup> *Id.*

<sup>34</sup> See Yahoo!, Inc. Form 10-K, *supra* note 2, at 47.

<sup>35</sup> Letter from Yahoo! Inc. to U.S. Sens. John Thune & Jerry Moran (Feb 23, 2017), available at <https://www.commerce.senate.gov/public/cache/files/ed55102d-33ae-406e-a700-b194cd6afcf/680BEF0769C55302BBA040C0BCE9E9D8.yahoo-letter.pdf>.

1           65. In its most recent 10-K filing with the SEC, Yahoo admits it had “contemporaneous  
2 knowledge” of the 2014 Breach, yet failed to “properly investigate[] and analyze[]” the breach, due  
3 in part to “failures in communication, management, inquiry and internal reporting” that led to a “lack  
4 of proper comprehension and handling” of the 2014 Breach.<sup>36</sup>

5           66. Adding insult to injury, Yahoo made no disclosures to its users about the breach—no  
6 email warnings, no public notices, and no communications. In fact, users heard nothing for two full  
7 years while Yahoo sat on this information and sophisticated identity thieves had free run of Class  
8 members’ PII and any confidential information that could be acquired by using that PII. Defendants’  
9 failure to take action and notify Class members also prevented unknowing Class members from  
10 taking action, thus leaving them even more vulnerable for a long period of time.

11           67. Sometime in 2015–2016 Yahoo’s data security was breached yet again. This time, the  
12 attack involved “forged cookies,” text files that Yahoo places on user computers when they log in so  
13 that users do not need to log in each time they start a new session. Authentication cookies contain  
14 information about the user’s session with Yahoo, and these cookies can contain a great deal of  
15 information about the user, such as whether that user has already authenticated to the company’s  
16 servers.<sup>37</sup>

17           68. The attackers in this case, presumed to be the same parties involved in the 2014  
18 Breach, were able to forge these authentication cookies, which granted them access to targeted  
19 accounts without needing to supply the account’s password. In addition, a forged cookie allowed the  
20 attackers to remain logged into the hacked accounts for weeks or indefinitely. Once again, there was  
21 no response from, or disclosure by, Yahoo.

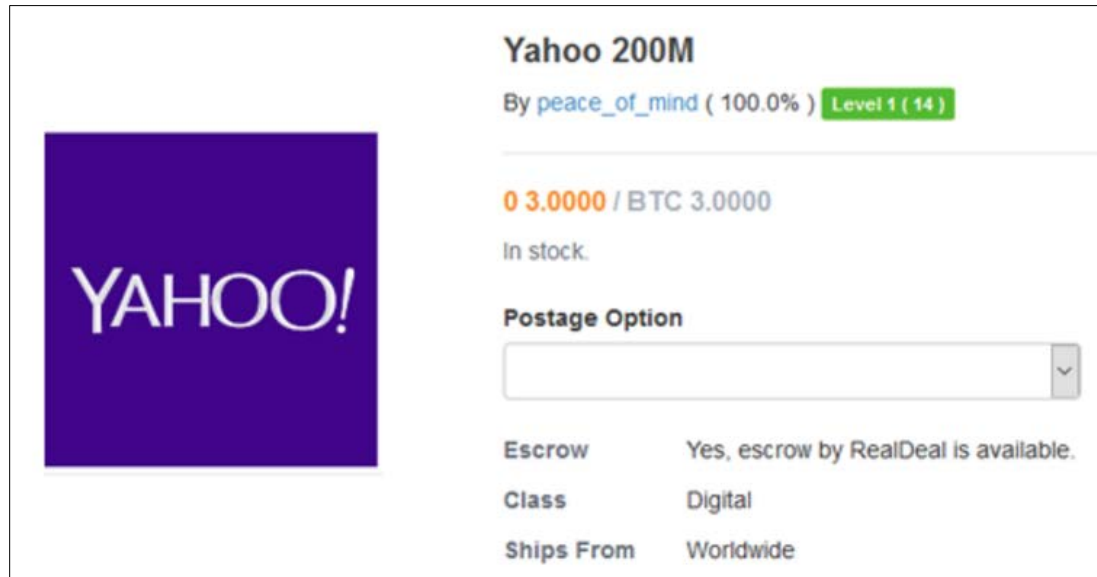
22           69. Meanwhile, without having disclosed any of these breaches, Yahoo solicited offers to  
23 buy the company. Reportedly, Yahoo wanted the offers in by April 19, 2016.<sup>38</sup>

24  
25  
26 <sup>36</sup> Yahoo!, Inc. Form 10-K, *supra* note 2, at 47.

27 <sup>37</sup> Krebs, *supra* note 28.

28 <sup>38</sup> David Goldman, Yahoo is for sale; bidders line up; Marissa Mayer is toast, CNN (Apr. 11, 2016, 10:29 AM), <http://money.cnn.com/2016/04/11/technology/yahoo-sale-marissa-mayer/>.

70. In August 2016, a hacker identifying himself or herself as “peace\_of\_mind” posted for sale on the dark web the PII from 200 million Yahoo accounts.



71. The Chief Intelligence Officer of Arizona cybersecurity company InfoArmor, who first spotted the massive database being offered for sale last August, told the *New York Times* in December 2016 that a geographically dispersed hacking group based in Eastern Europe managed to sell copies of the database to three buyers for \$300,000 apiece months before Yahoo disclosed the 2014 Breach.<sup>39</sup>

72. Yahoo responded to media inquiries about this by noting that it was “‘aware’ of the hacker’s claims, but ha[d] not confirmed nor denied the legitimacy of the data” offered for sale.<sup>40</sup>

#### F. Yahoo Reveals the 2014 Breach Years After It Happened

73. Finally, on September 22, 2016, more than 3 years after the largest breach (the 2013 Breach), Yahoo publicly announced that the 2014 Breach had occurred. Yahoo said in a statement

<sup>39</sup> Jordan Robertson, Stolen Yahoo Data Includes Government Employee Information, Bloomberg Technology (Dec. 14, 2016, 6:09 PM), <https://www.bloomberg.com/news/articles/2016-12-15/stolen-yahoo-data-includes-government-employee-information>; Lisa Vaas, Yahoo breach: your account is selling for pennies on the dark web, naked security (Dec. 20, 2016), <https://nakedsecurity.sophos.com/2016/12/20/yahoo-breach-your-account-is-selling-for-pennies-on-the-dark-web/>.

<sup>40</sup> Joseph Cox, Yahoo ‘Aware’ Hacker Is Advertising 200 Million Supposed Accounts on Dark Web, MOTHERBOARD (Aug. 1, 2016), <http://motherboard.vice.com/read/yahoo-supposed-data-breach-200-million-credentials-dark-web>.

1 that “the account information may have included names, email addresses, telephone numbers, dates  
 2 of birth, hashed passwords (the vast majority with bcrypt) and, in some cases, encrypted or  
 3 unencrypted security questions and answers.”<sup>41</sup> This announcement came just two months after  
 4 Yahoo announced Verizon’s plan to acquire its operating assets, and just weeks after Yahoo reported  
 5 to the SEC that it knew of no incidents of unauthorized access of personal data that might adversely  
 6 affect the potential acquisition.<sup>42</sup>

7 74. Incredulously, Yahoo also claimed it did not uncover the 2014 Breach for two years,  
 8 a claim met with immediate skepticism. A September 23, 2016 *Financial Times* report stated that  
 9 “Yahoo CEO Marissa Mayer has known that Yahoo was investigating a serious data breach since  
 10 July, but withheld the information from investors, regulators and acquirer Verizon until this  
 11 week...”<sup>43</sup> Only later would Yahoo concede it knew about the 2014 Breach at the time it took place.

12 75. Yahoo had reason to keep any breach under wraps. It struggled for years to compete  
 13 with more successful technology giants and is now in the midst of a sale of its operating assets and  
 14 businesses to Verizon for billions of dollars. By intentionally failing to disclose the breach in a  
 15 timely manner as required by law, Yahoo misled consumers into continuing to sign up for Yahoo  
 16 services and products, thus providing Yahoo a continuing income stream and a better chance of  
 17 finalizing a sale of the company to Verizon. Yahoo’s CEO Marissa Mayer alone was estimated to  
 18 make almost \$123 million from the sale of Yahoo assets to Verizon.<sup>44</sup>

---

22  
 23 <sup>41</sup> Yahoo Security Notice September 22, 2016, Yahoo! Help, <https://help.yahoo.com/kb/SLN28092.html> (last visited Apr 9, 2017).

24 <sup>42</sup> Kurt R. Hunt, Timing Is Everything in Data Breach Investigations and Disclosures: Yahoo  
 25 Breach, The National Law Review (Nov. 2, 2016), <http://www.natlawreview.com/article/timing-everything-data-breach-investigations-and-disclosures-yahoo-breach>.

26 <sup>43</sup> Harriett Taylor, Yahoo CEO Mayer knew about data breach in July: Report, CNBC (Sept. 23,  
 27 2016, 3:51 PM), <http://www.cnbc.com/2016/09/23/yahoo-ceo-mayer-knew-about-data-breach-in-july-report.html>.

28 <sup>44</sup> Stephen Gandel, Marissa Mayer’s Payday Is Even More Insane Than You Think, FORTUNE (July 26, 2016), <http://fortune.com/2016/07/26/marissa-mayers-verizon-yahoo-pay/>.



76. Yahoo's lack of timely, legally-mandated disclosure upset several United States senators. On September 27, 2016, after Yahoo's belated disclosure of the 2014 Breach, six senators sent Yahoo CEO Marissa Mayer the below letter, which outlined several concerns. Particularly troubling to the senators was Yahoo's failure to notify its users of the 2014 Breach sooner.

**United States Senate**  
WASHINGTON, DC 20510

September 27, 2016

Ms. Marissa Mayer  
Chief Executive Officer  
Yahoo Inc.  
701 First Avenue  
Sunnyvale, CA 94089

Dear Ms. Mayer:

We write following your company's troubling announcement that account information for more than 500 million Yahoo users was stolen by hackers, compromising users' personal information across the Yahoo platform and on its sister sites, including Yahoo Mail, Flickr, Yahoo Finance, and Yahoo Fantasy Sports. The stolen data included usernames, passwords, email addresses, telephone numbers, dates of birth, and security questions and answers. This is highly sensitive, personal information that hackers can use not only to access Yahoo customer accounts, but also potentially to gain access to any other account or service that users access with similar login or personal information, including bank information and social media profiles.

We are even more disturbed that user information was first compromised in 2014, yet the company only announced the breach last week. That means millions of Americans' data may have been compromised for two years. This is unacceptable. This breach is the latest in a series of data breaches that have impacted the privacy of millions of American consumers in recent years, but it is by far the largest. Consumers put their trust in companies when they share personal and sensitive information with them, and they expect all possible steps be taken to protect that information.

77. The Plaintiffs and the Class are informed and believe that investigations by the Senate, the Department of Justice, and the Securities and Exchange Commission into Yahoo's failure to disclose the breaches sooner remain ongoing.



**G. More Than Three Years After the Fact, Yahoo Finally Acknowledges the 2013 Breach**

78. On December 14, 2016, Yahoo finally admitted to the 2013 Breach. Yahoo's Chief Information Security Officer posted the following under an announcement titled "Important Security Information for Yahoo Users":

As we previously disclosed in November, law enforcement provided us with data files that a third party claimed was Yahoo user data. We analyzed this data with the assistance of outside forensic experts and found that it appears to be Yahoo user data. Based on further analysis of this data by the forensic experts, we believe an unauthorized third party, in August 2013, stole data associated with more than one billion user accounts. We have not been able to identify the intrusion associated with this theft.<sup>45</sup>

79. In addition to catching the attention of the international media and several governments, these revelations caused Verizon, which was poised to buy Yahoo's operating assets and businesses for \$4.83 billion, to demand a \$925 million discount on the purchase price. Ultimately, the parties agreed on a \$350 million price reduction and an adjustment regarding the parties' respective shares of liability and litigation costs.<sup>46</sup>

**H. Despite All of This, Yahoo *Still* Waits to Notify Users Affected by the Forged Cookie Breach**

80. Yahoo quietly divulged the Forged Cookie Breach in its 10-Q filing with the SEC filed November 9, 2016.<sup>47</sup> While filed publicly, the two brief references in the 141-page filing were overshadowed by the ongoing coverage of the 2014 Breach. Yahoo declined to notify any affected users at that time.

81. Not until February 2017 did Yahoo begin notifying account holders that their email accounts may have been accessed without the need for a password resulting from the use of forged

<sup>45</sup> Bob Lord, Important Security Information for Yahoo Users, Yahoo! Tumblr (Dec. 14, 2016), <https://yahoo.tumblr.com/post/154479236569/important-security-information-for-yahoo-users>.

<sup>46</sup> Michael Liedtke, Verizon asked for \$925M discount for Yahoo data breaches, The Star (Mar. 13, 2017), <https://www.thestar.com/business/2017/03/13/verizon-asked-for-925m-discount-for-yahoo-data-breaches.html>.

<sup>47</sup> Yahoo!, Inc. 2016 Form 10-Q for quarterly period ended Sept. 30, 2016 (Nov. 9, 2016), at 40, 69, <https://investor.yahoo.net/secfiling.cfm?filingID=1193125-16-764376&CIK=1011006>.

cookies. According to Yahoo, the Forged Cookie Breach was related to the 2014 Breach.<sup>48</sup> Yahoo's notification informed affected users that "a forged cookie may have been used in 2015 or 2016 to access your account."<sup>49</sup>

82. Yahoo claimed that, since discovering the breach, it had "invalidated the forged cookies and hardened [its] systems to secure them against similar attacks."<sup>50</sup> Yet, users affected by the Forged Cookie Breach were not notified until many months after Yahoo had discovered it.<sup>51</sup>

83. Again, data security experts were aghast. One expert, Brian Krebs, saw the Forged Cookie Breach as yet more evidence that Yahoo's online services are unusable<sup>52</sup>:

**Q: That sounds pretty bad.**

A: Yeah, that's about as bad as it gets. It's yet another reason I'm telling people to run away from Yahoo email.

#### **I. The Full Extent of the Fallout from the Breaches is Not Yet Known**

84. Unfortunately, for the victims of these Yahoo Data Breaches, their stolen information was still for sale on underground hacker forums as late as March 17, 2017.<sup>53</sup> Their PII will be indefinitely available to those who are willing to pay for it as evidenced by the multiple databases for sale online, as shown on the following page.

<sup>48</sup> Mike Snider & Elizabeth Weise, Yahoo notifies users of 'forged cookie' breach, USA Today (Feb. 15, 2017, 3:59 PM), <http://www.usatoday.com/story/tech/news/2017/02/15/yahoo-notifies-users-forged-cookie-breach/97955438/>.

<sup>49</sup> *Id.*

<sup>50</sup> Gareth Halfacree, Yahoo warning users of forged cookie account attacks, bit-tech (Feb. 17, 2017), <https://www.bit-tech.net/news/bits/2017/02/17/yahoo-warning-forged-cookies/1>.

<sup>51</sup> Michelle Castillo, Yahoo's new hack warning comes from a third breach, the company says, CNBC (Feb. 15, 2017, 1:38 PM), <http://www.cnbc.com/2017/02/15/yahoo-sends-new-warning-to-customers-about-data-breach.html>.

<sup>52</sup> Krebs, *supra* note 28.

<sup>53</sup> Vindu Goel, One Billion Yahoo Accounts Still for Sale, Despite Hacking Indictments, The New York Times (Mar. 17, 2017), <https://www.nytimes.com/2017/03/17/technology/yahoo-hack-data-indictments.html>.

Home / Digital Goods / Leaks & Databases / Yahoo | 100K | Email:Pass | Decrypted | Instant Delivery



**Yahoo | 100K | Email:Pass | Decrypted | Instant Delivery**

USD 10.50 (including 0.51 transaction fee)  
฿ 0.0097

**In stock**

Vendor: SunTzu583 [+31] [-2] Level 4 (80+)

Class: Digital

Delivery: Instant Delivery

Also available:


Yahoo   135,754   Email:Pass   Decrypted   Instant Delivery	USD 13.60 ฿ 0.0120
---	--------------------

Quantity: 1

**Buy Now**

? Question Report

Home / Digital Goods / Leaks & Databases / Yahoo | 5,737,977 | Decrypted | Complete | Instant Delivery



**Yahoo | 5,737,977 | Decrypted | Complete | Instant Delivery**

USD 240.50 (including 0.51 transaction fee)  
฿ 0.2330

**In stock**

Vendor: SunTzu583 [+31] [-2] Level 4 (80+)

Class: Digital

Delivery: Instant Delivery

Also available:

Yahoo   1,912,659   Decrypted   Part 1   Instant Delivery	USD 100.50 ฿ 0.0948
Yahoo   1,912,659   Decrypted   Part 2   Instant Delivery	USD 100.50 ฿ 0.0948
Yahoo   1,912,658   Decrypted   Part 3   Instant Delivery	USD 100.50 ฿ 0.0948

Quantity: 1

**Buy Now**

? Question Report

**Details** **Feedback**

## Listing Details

This is the complete list containing all the three Yahoo parts.

This list is 5,737,977 rows long. Every row contains an Yahoo email and a password. There are no duplicate lines. So all rows are unique.

Preview of List:

```

[REDACTED]@yahoo.com:[REDACTED]
[REDACTED]@yahoo.com:[REDACTED]
[REDACTED]@yahoo.com:[REDACTED]
[REDACTED]@yahoo.com:[REDACTED]
[REDACTED]@yahoo.com:[REDACTED]
[REDACTED]@yahoo.com:[REDACTED]
[REDACTED]@yahoo.com:[REDACTED]
[REDACTED]@yahoo.com:[REDACTED]
  
```

85. Making the situation for Class members even worse, Yahoo does not make it easy to delete user email accounts. Although the process may appear straightforward enough, users have to wait at least 90 days after requesting deletion for it to take effect. And even then, the account often remains active. For example, one user tried to delete his Yahoo account, waited 90 days and on the 91st day checked to see if the account was still active. Unfortunately, and as confirmed by Yahoo, his act of trying to log in to make sure the account was inactive reset the 90-day clock.<sup>54</sup> Other users have also noted that their accounts remained active long after the 90-day period even though they have not logged in.<sup>55</sup>

86. The Data Breaches have had internal effects at Yahoo as well. In Yahoo's 10-K filing with the SEC, Yahoo disclosed that an independent committee of Yahoo's Board of Directors had investigated the Data Breaches and determined that Yahoo's information security team knew, at a minimum, about the 2014 Breach and the Forged Cooke Breach as they were happening, but took no real action in the face of that knowledge.<sup>56</sup>

87. With this admission, Yahoo decided it needed a sacrificial lamb, and that person was Ronald Bell, Yahoo's General Counsel. After the independent committee also determined that the Yahoo legal team "had sufficient information to warrant substantial further inquiry in 2014, and they did not sufficiently pursue it," Bell allegedly "resigned" from his position. Yahoo's 10-K notes that "no payments are being made to Mr. Bell in connection with his resignation."<sup>57</sup> In other words, he received no severance payment.

---

<sup>54</sup> Zack Whittaker, Deleting your Yahoo email account? Yeah, good luck with that, ZDNet (Feb. 17, 2017, 10:00 PM), <http://www.zdnet.com/article/yahoo-not-deleting-email-accounts-say-users/>.

<sup>55</sup> *Id.*

<sup>56</sup> See Yahoo!, Inc. Form 10-K, *supra* note 2, at 46-47.

<sup>57</sup> *Id.* at 47.

1           88. Analysts saw Bell’s resignation  
2 for what it was—a feeble attempt to create  
3 accountability by terminating someone who  
4 was not the policy-maker at Yahoo. Yahoo’s  
5 former head of media, Scott Moore, found the  
6 situation “ridiculous”:



Scott Moore  
@scottm00re

Follow

Ridiculous. I know @ronsbelt\_tech who is a good man and as a lawyer he wasn't in charge of security @Yahoo #ame CYA move @marissamayer twitter.com/karaswisher/st...  
4:25 PM - 1 Mar 2017

16 36

7           89. In addition, Yahoo’s board of directors, “[i]n response to the Independent  
8 Committee’s findings related to the 2014” breach, elected not to award CEO Marissa Mayer her  
9 2016 cash bonus, and Mayer has supposedly “offered to forgo any equity award in 2017 given that  
10 the 2014 Security Incident occurred during her tenure.”<sup>58</sup>

11           90. The 2014 Breach and Forged Cookie Breach have since been attributed to two  
12 Russian FSB agents, a Russian hacker, and a Canadian hacker. A Justice Department spokesperson  
13 said of the breaches, “FSB officers used criminal hackers to gain information that clearly ... has  
14 intelligence value,” and “the criminal hackers used the opportunity to line their own pockets.”<sup>59</sup>

15           91. On information and belief, the 2014 breach began with a “spear phishing” email  
16 campaign sent to upper-level Yahoo employees.<sup>60</sup> One or more of these employees fell for the bait,  
17 and Yahoo’s data security was so lax, that this action was enough to hand over the proverbial keys to  
18 the kingdom.

19           92. The hackers then managed to infiltrate Yahoo’s “User Database” (“UDB”), a  
20 database containing PII about all Yahoo users, including account names, recovery email accounts  
21 and phone numbers, password challenge questions and answers, and the account “nonce,” a  
22

23 <sup>58</sup> *Id.*

24 <sup>59</sup> Indictment, United States v. Dokuchaev et al. (Feb. 28, 2017), ¶¶ 22-23, 3:17-cr-00103, ECF No.  
25 1; Del Quentin Wilbur & Paresh Dave, Justice Department charges Russian spies, hackers in  
26 massive Yahoo breach, Chicago Tribune (Mar. 15, 2017, 3:39 PM), <http://www.chicagotribune.com/news/nationworld/ct-russia-yahoo-hacks-20170315-story.html>.

27 <sup>60</sup> Indictment, *supra* note 59; *see also* Swati Khandelwal, Yahoo! Hack! How It Took Just One-Click  
28 to Execute Biggest Data Breach in History, The Hacker News (Mar. 15, 2017), <https://thehackernews.com/2017/03/yahoo-data-breach-hack.html>.

1 cryptographic value unique to the targeted victim account. They then downloaded the contents of  
 2 this database on to their own systems. The hackers also gained access to the Account Management  
 3 Tool (“AMT”), a tool that allowed Yahoo to manage all aspects of its users’ accounts, including  
 4 making, logging, and tracking changes in the account, such as password changes.<sup>61</sup>

5 93. With these tools, the hackers were able to target all kinds of sources, including  
 6 specific personal targets and general searches such as credit card verification values (“cvv”  
 7 numbers), and terms such as “credit card,” “amex,” “visa,” “mastercard,” “gift card,” and others.<sup>62</sup>

8 94. Further, the hackers also used the Yahoo UDB information to compromise related  
 9 user accounts with cloud-based services like Apple and webmail providers like Google.<sup>63</sup>

10 95. Finally, the hackers were able to use the “nonces” to generate forged cookies so that  
 11 they could gain continuous access to user accounts without having to re-enter password or other  
 12 security information.<sup>64</sup>

13 96. Although Yahoo claims to have plugged the leaks, any fix does not address the issue  
 14 of Yahoo users’ PII being currently in the hands of these hackers. Yahoo users whose PII has been  
 15 unlawfully accessed or stolen should sign up for credit protection services immediately. Such  
 16 services cost money, however. For example, according to the California Department of Justice, the  
 17 three main credit bureaus charge \$10 each to “freeze” credit files.<sup>65</sup> Yahoo has yet to offer to  
 18 reimburse such costs for the millions of users affected by the Yahoo Data Breaches.

#### 19 **J. Yahoo’s Small Business Customers Depended on Defendants’ PII Security Practices**

20 97. Defendants Yahoo and Aabaco understand that online security is paramount to their  
 21 Small Business customers and was highly material to their decision to utilize Defendants’ Small  
 22 Business services. Defendants address these concerns in the advertising that Defendants present to  
 23

---

24 <sup>61</sup> Indictment, *supra* note 59, ¶¶ 22-33; *see also* Martyn Williams, Inside the Russian hack of Yahoo:  
 25 How they did it, CSO (March 16, 2017, 4:29 AM), [http://www.csoonline.com/article/3180762/data-](http://www.csoonline.com/article/3180762/data-breach/inside-the-russian-hack-of-yahoo-how-they-did-it.html)  
 26 breach/inside-the-russian-hack-of-yahoo-how-they-did-it.html.

<sup>62</sup> Indictment, *supra* note 59, ¶¶ 22-33.

<sup>63</sup> *Id.*

<sup>64</sup> *Id.*

<sup>65</sup> How to “Freeze” Your Credit Files, Cal. Dept. of Justice, [https://www.oag.ca.gov/idtheft/](https://www.oag.ca.gov/idtheft/facts/freeze-your-credit)  
 28 facts/freeze-your-credit (lasted visited Apr. 5, 2017).



all would-be customers exploring the Small Business services. All customers, including Plaintiff Neff, were exposed to and read these advertisements and explanations, which appear on the webpages all customers must use to sign-up for the services.

98. This 2009 advertisement and explanation page for the web hosting services utilized by Plaintiff Neff, found under the “security” tab, touts: “It’s easy to create a professional-looking website. Reassure customers with the VeriSign Verified™ Seal.”

99. The current web hosting advertisement and explanations page similarly assures that web hosting is safe and secure, highlighting the following points<sup>66</sup>:

## Grow your business with a web site from Yahoo! Web Hosting.



## Web Hosting features



### Secure and reliable

- Web Hosting sites are up and running 99.9% of the time.
- Your website is backed up in different geographic locations so it will stay live in an emergency.
- Your website runs on a Unix operating system and Apache servers.
- Password protection is available for your accounts and sections of your website (Advanced and Premier plans only).
- Shared SSL certificates and encryption protect the information customers submit to your site (Advanced and Premier plans only).

<sup>66</sup> Flexible hosting for your professional website, Yahoo! Aabaco Small Business, <https://smallbusiness.yahoo.com/webhosting#reliable> (last visited Apr. 12, 2017).



100. The relationship between Defendants and Small Business Class Members is governed by Defendants' Terms of Service, which incorporate by reference a number of other agreements including Defendants' Privacy Policy ("Privacy Policy"). Throughout the relevant time, the Terms of Service was a "click-through" agreement. Each member of the Small Business Users Class, including Plaintiff Neff, prior to becoming a Small Business customer, was required to click a box stating that "I agree to the terms of service," with terms of service being a live link page that would open when clicked.<sup>67</sup>

101. The Terms of Service expressly refer to both Aabaco and Yahoo<sup>68</sup>:

### Terms of Service

< Terms of Service Center

This website and the services and products offered are provided by Aabaco Small Business, LLC and its subsidiaries (the "Company") subject to the following Terms of Service ("Terms"), which may be updated from time to time without notice to the user ("You", "Your", or "Merchant"). The Company is a wholly-owned subsidiary of Yahoo! Inc ("Yahoo"). By accessing and using this website and the services and products offered on it, You accept and agree to be bound by the Terms. In addition, when using this website, the services, or products, You will be subject to any posted guidelines or rules applicable to such services, which may be posted and modified from time to time. All such guidelines and rules, including the Privacy Policy, the Site Guidelines, and certain third party agreements as described below, are hereby incorporated by reference into these Terms (all together, the "Agreement").

102. The Privacy Policy has been updated over the years but, as relevant to this action, has always contained identical or substantively similar assurances that Defendants appropriately safeguard the PII entrusted to them.<sup>69</sup> The Privacy Policy in effect throughout the relevant time represents that:

### CONFIDENTIALITY AND SECURITY

We limit access to Personal Information about You to employees, contractors, or service providers who we believe reasonably need to come into contact with that information to provide products or services to You or in order to do their jobs.

We have physical, electronic, and procedural safeguards that comply with federal regulations to protect Personal Information about You.

<sup>67</sup> Account Creation and Login Page, Yahoo! Aabaco Small Business, <https://login.luminate.com/registration?.src=smbiz&.done=https%3A%2F%2Fwww.luminate.com> (last visited Apr. 5, 2017).

<sup>68</sup> Terms of Service, Yahoo! Aabaco Small Business, <https://smallbusiness.yahoo.com/tos> (last visited Apr. 5, 2017).

<sup>69</sup> Privacy Policy, Yahoo! Aabaco Small Business, <https://www.aabacosmallbusiness.com/privacy-policy?updated=true> (last visited Apr. 5, 2017).

103. In addition, the Privacy Policy represents that Defendants do not share PII except in the following delineated circumstances<sup>70</sup>:

#### INFORMATION SHARING AND DISCLOSURE

The Company does not rent, sell, or share Personal Information about You with other people or non-affiliated companies except to provide products or services You've requested, when we have Your permission, or under the following circumstances:

- **Service Providers, Contractors, and Agents:** We provide information to partners who work on behalf of or with the Company under confidentiality agreements. These companies do not have any independent right to share this information.
- **Co-Branded Partners:** The Company may provide some services in partnership with others under a co-branded experience. In these situations both companies may be collecting information about You so please see the privacy links available within the experience to learn more. For example, Business Mail is provided in partnership with Yahoo.
- **Legal Process:** We respond to subpoenas, court orders, or legal process, or to establish or exercise our legal rights or defend against legal claims.
- **Security & Fraud:** We believe it is necessary to share information in order to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of the Terms of Service, or as otherwise required by law.
- **Merger & Acquisition:** We transfer information about You if the Company is acquired by or merged with another company.

104. As Plaintiff Neff and the members of the Small Business Users Class would discover in 2016, these material representations about security were false and misleading because Defendants failed to disclose that their Small Business services were not secure, and that the PII they would be entrusting to Defendants was not reasonably safeguarded.

#### CLASS ACTION ALLEGATIONS

105. Pursuant to Rule 23(b)(2), (b)(3) and (c)(4) of the Federal Rules of Civil Procedure, Plaintiffs, individually and on behalf of all others similarly situated, bring this lawsuit on behalf of themselves and as a class action on behalf of the following classes:

##### **A. The United States Class**

All persons or businesses who registered for Yahoo accounts (other than Yahoo Small Business or Aabaco accounts) in the United States and

---

<sup>70</sup> *Id.*

whose PII was accessed, compromised, or stolen from Yahoo in the 2013 Breach, the 2014 Breach, or the Forged Cookie Breach.

**B. The Small Business Users Class**

All persons or businesses who registered for Yahoo Small Business or Aabaco accounts in the United States and whose PII was accessed, compromised, or stolen from Yahoo or Aabaco in the 2013 Breach, the 2014 Breach, or the Forged Cookie Breach.

**C. The Australia, Venezuela, and Spain Class**

All persons or businesses who registered for Yahoo accounts in the countries of Australia, Venezuela, and Spain and whose PII was accessed, compromised, or stolen from Yahoo in the 2013 Breach, the 2014 Breach, or the Forged Cookie Breach.

**D. The Israel Class**

All persons or businesses who registered for Yahoo accounts in the country of Israel and whose PII was accessed, compromised, or stolen from Yahoo in the 2013 Breach, the 2014 Breach, or the Forged Cookie Breach.

106. Collectively, all of the classes will be referred to herein as the “Class,” except where otherwise noted in order to differentiate them.

107. Excluded from the Class are Defendants and any entities in which any Defendant or their subsidiaries or affiliates have a controlling interest, and Defendants’ officers, agents, and employees.

108. **Numerosity:** The members of each Class are so numerous that joinder of all members of any Class would be impracticable. Plaintiffs reasonably believe that Class members number hundreds of millions of people or more in the aggregate and well over 1,000 in the smallest of the classes. The names and addresses of Class members are identifiable through documents maintained by Defendants.

109. **Commonality and Predominance:** This action involves common questions of law or fact, which predominate over any questions affecting individual Class members, including:

A. For All Classes:

- i. Whether Defendants represented to the Class that they would safeguard Class members' PII;
- ii. Whether Defendants owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII;
- iii. Whether Defendants breached a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII;
- iv. Whether Class members' PII was accessed, compromised, or stolen in the 2013 Breach;
- v. Whether Class members' PII was accessed, compromised, or stolen in the 2014 Breach;
- vi. Whether Class members' PII was accessed, compromised, or stolen in the Forged Cookie Breach;
- vii. Whether Defendants knew about any or all of the Breaches before they were announced to the public and failed to timely notify the public of those Breaches;
- viii. Whether Plaintiffs and the other Class members are entitled to actual, statutory, or other forms of damages, and other monetary relief; and
- ix. Whether Plaintiffs and the Class are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

B. For the United States Class, Small Business Users Class and Israel Classes

- i. Whether Defendants' conduct violated Cal. Civ. Code § 1750, *et seq.*;
- ii. Whether Defendants' conduct was an unlawful or unfair business practice under Cal. Bus. & Prof. Code § 17200, *et seq.*;
- iii. Whether Defendants' conduct violated Cal. Civ. Code § 1798.80 *et seq.*;
- iv. Whether Defendants' conduct violated Cal. Bus. & Prof. Code § 22575, *et seq.*, and

v. Whether Defendants' conduct violated the Stored Federal Stored Communications Act, 18 U.S.C. § 2702.

C. For the Australia, Venezuela, and Spain Class

i. Whether Defendants negligently or recklessly breached legal duties owed to Plaintiffs and the Australia, Venezuela, and Spain Classes to exercise due care in collecting, storing, and safeguarding their personal and financial information.

110. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs individually and on behalf of the members of their respective classes. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous common questions that dominate this action.

111. **Typicality:** Plaintiffs' claims are typical of the claims of the other members of their respective classes because, among other things, Plaintiffs and the other class members were injured through the substantially uniform misconduct by Defendants. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of other Class members arise from the same operative facts and are based on the same legal theories.

112. **Adequacy of Representation:** Plaintiffs are adequate representatives of the classes because their interests do not conflict with the interests of the other Class members they seek to represent; they have retained counsel competent and experienced in complex class action litigation and Plaintiffs will prosecute this action vigorously. The Class members' interests will be fairly and adequately protected by Plaintiffs and their counsel.

113. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiffs and the other members of their respective classes are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendants, making it impracticable for Class members to individually seek

1 redress for Defendants' wrongful conduct. Even if Class members could afford individual litigation,  
 2 the court system could not. Individualized litigation would create a potential for inconsistent or  
 3 contradictory judgments, and increase the delay and expense to all parties and the court system. By  
 4 contrast, the class action device presents far fewer management difficulties and provides the benefits  
 5 of single adjudication, economies of scale, and comprehensive supervision by a single court.

6 114. Further, Defendants have acted or refused to act on grounds generally applicable to  
 7 the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the  
 8 members of the Class as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil  
 9 Procedure.

10 115. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification  
 11 because such claims present only particular, common issues, the resolution of which would advance  
 12 the disposition of this matter and the parties' interests therein. Such particular issues include, but are  
 13 not limited to:

- 14 a. Whether Class members' PII was accessed, compromised, or stolen in the  
 15 2013 Breach;
- 16 b. Whether Class members' PII was accessed, compromised, or stolen in the  
 17 2014 Breach;
- 18 c. Whether Class members' PII was accessed, compromised, or stolen in the  
 19 Forged Cookie Breach;
- 20 d. Whether (and when) Defendants knew about any or all of the Breaches before  
 21 they were announced to the public and failed to timely notify the public of  
 22 those Breaches;
- 23 e. Whether Defendants owed a legal duty to Plaintiffs and the Class to exercise  
 24 due care in collecting, storing, and safeguarding their PII;
- 25 f. Whether Defendants breached a legal duty to Plaintiffs and the Class to  
 26 exercise due care in collecting, storing, and safeguarding their PII;
- 27 g. Whether Defendants' conduct was an unlawful or unfair business practice  
 28 under Cal. Bus. & Prof. Code § 17200, *et seq.*;



- h. Whether Defendants' representations that they would secure and protect the PII and financial information of Plaintiffs and members of the classes were facts that reasonable persons could be expected to rely upon when deciding whether to use Defendants' services;
- i. Whether Defendants misrepresented the safety of their many systems and services, specifically the security thereof, and their ability to safely store Plaintiffs' and Class members' PII;
- j. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;
- k. Whether Plaintiffs and the other class members are consumers within the meaning of Cal. Civ. Code §1761(d);
- l. Whether Defendants' acts, omissions, misrepresentations, and practices were and are likely to deceive consumers;
- m. Whether Defendants knew or should have known that they did not employ reasonable measures to keep Plaintiffs' and Class members' PII or financial information secure and prevent the loss or misuse of that information;
- n. Whether Defendants' conduct violated Cal. Civ. Code § 1798.80 *et seq.*;
- o. Whether Defendants' conduct violated the Stored Federal Stored Communications Act ("SCA"), 18 U.S.C. § 2702;
- p. Whether Defendants provide an "electronic communication service to the public" within the meaning of the SCA;
- q. Whether Defendants provide remote computing services to the public by virtue of their computer processing services for electronic communications;
- r. Whether Defendants failed to take commercially reasonable steps to safeguard the PII and sensitive financial information of Plaintiffs and the Class members and thereby knowingly divulged the PII and sensitive financial information of Plaintiffs and the Class members while in electronic storage in Defendants'

1 system and/or while carried and maintained on Defendants' remote computing  
2 service;

3 s. Whether Defendants' conduct violated Cal. Bus. & Prof. Code § 22575, *et*  
4 *seq.*;

5 t. Whether Defendants are a commercial website or online service that collects  
6 personally identifiable information through the Internet about individual  
7 consumers residing in California, and elsewhere, who use or visit its  
8 commercial Web site or online services, within the meaning of California  
9 Business and Professions Code § 22575(a);

10 u. Whether Defendants failed to adhere to their posted privacy policy concerning  
11 the care they would take to safeguard Plaintiffs' and Class members' PII in  
12 violation of California Business and Professions Code § 22576;

13 v. Whether Defendants negligently and materially failed to adhere to their posted  
14 privacy policy with respect to the extent of their disclosure of users' data, in  
15 violation of California Business and Professions Code § 22576;

16 w. Whether a contract existed between Defendants and Plaintiffs and the Class  
17 members, and the terms of that contract;

18 x. Whether Defendants breached the contract by having inadequate safeguards;

19 y. Whether an implied contract existed between Defendants and Plaintiffs and  
20 the Class members and the terms of that implied contract;

21 z. Whether Defendants breached the implied contract;

22 aa. Whether Defendants violated the covenant of good faith and fair dealing  
23 implicit in such contract;

24 bb. Whether Defendants made representations regarding the supposed secure  
25 nature of their small business services;

26 cc. Whether such representations were false with regard to storing and  
27 safeguarding Class members' PII; and  
28

dd. Whether such representations were material with regard to storing and safeguarding Class members' PII.

### **CHOICE OF LAW**

116. Members of the United States Class, all of whom registered for Yahoo accounts in the United States, were required as a condition of using Yahoo's services to agree to Yahoo's Terms of Service. This was a "clickwrap" agreement where members of the United States Class had to affirmatively accept the Terms.

117. Among other provisions, Yahoo's Terms of Service for the United States Class have a forum selection clause and choice of law clause. The pertinent language reads:

The Agreement and the relationship between You and the Company **shall be governed by the laws of the State of California without regard to its conflict of law provisions**, and specifically excluding from application to this Agreement that law known as the United Nations Convention on the International Sale of Goods. You and the Company agree to submit to the personal jurisdiction of the courts located within the county of Santa Clara, California. The failure of the Company to exercise or enforce any right or provision of this Agreement shall not constitute a waiver of such right or provision.

118. In accordance with the choice of law provision, Yahoo has stipulated that California common law and statutory law applies to all claims by members of the United States Class.

119. Members of the Small Business Users Class, all of whom registered for Yahoo Small Business or Aabaco accounts in the United States, were required as a condition of using those services to agree to Terms of Service. This was a "clickwrap" agreement where members of the United States Class had to affirmatively accept the Terms.

120. Among other provisions, Aabaco's Terms of Service have a forum selection clause and choice of law clause. The pertinent language reads:

### **CHOICE OF LAW AND FORUM (LOCATION OF LAWSUIT)**

The Agreement and the relationship between You and the Company shall be **governed by the laws of the State of California without regard to its conflict of law provisions**, and specifically excluding from application to this Agreement that law known as the United Nations Convention on the International Sale of Goods. You and the Company agree to submit to the

personal jurisdiction of the courts located within the county of Santa Clara, California.

121. The members of the Israel Class agreed to Yahoo's Terms of Service for Israel, which provide that:

If you are using...Israeli (il) Services, you are contracting with Yahoo! Inc., 701 First Avenue, Sunnyvale, CA 94089 to provide you with the Services and the **substantive law of the State of California governs the interpretation of this ATOS [] and applies to all claims related to it, regardless of the conflict of laws principles.** You and Yahoo! Inc., irrevocably consent to the exclusive jurisdiction and venue of the state courts located in Santa Clara County, California or in the Federal Courts located in the Northern District of California, USA for all disputes arising out of or relating to this ATOS or arising out of or relating to the relationship between you and Yahoo regardless of the type of claim.

122. Class members who signed up for Yahoo services in Australia, Venezuela, and Spain did not contract directly with Yahoo. Instead, they contracted with various foreign Yahoo subsidiaries, many of which had differing Terms of Service. But, as those subsidiaries are not parties to this litigation and, as the Australia, Venezuela, and Spain Classes are alleging wrongdoing only on the part of Yahoo, Inc. and Aabaco, those Terms of Service do not govern the choice of law or venue analyses for those Class members.

123. Also, those terms of service specifically inform users that PII they provide to Yahoo Subsidiaries in order to open their accounts will be routed through Yahoo's United States-based servers. For instance, Yahoo users who registered for Yahoo services in Australian agreed to terms of service that state:

When you register with Yahoo7, you acknowledge that in using Yahoo7 services to send electronic communications (including but not limited to email, search queries, sending messages to Yahoo7 Services and other Internet activities), you will be causing communications to be sent through Yahoo7's computer networks, portions of which are located in California, Texas, Virginia, and other locations in the United States and portions of which are located in other countries.<sup>71</sup>

---

<sup>71</sup> Yahoo7 Terms of Service, Yahoo7, <https://policies.yahoo.com/au/en/yahoo/terms/utos/index.htm> (last visited Apr. 8, 2017).

1 Under the section entitled “Yahoo Privacy Policy,” the terms of service continue:

2 Registration Data and certain other information about you is subject to our  
3 Privacy Policy. You understand that through your use of the Service you  
4 consent to the collection and use (as set forth in the Privacy Policy) of this  
5 information, including the transfer of this information to the United States  
6 and/or other countries for storage, processing and use by Yahoo7 and its  
7 affiliates.<sup>72</sup>

8 124. Similarly, Yahoo users who registered for Yahoo services in Spain agreed to terms of  
9 service and incorporated privacy policy that state, “Your personal information may be transferred to  
10 other countries, especially servers located in the United States, to process and store data in  
11 accordance with our Privacy Policy and to offer you some of our products and services.”<sup>73</sup>

12 125. Moreover, because Defendants are headquartered in California and all of their key  
13 decisions and operations emanate from California, California law can and should apply to claims  
14 relating to the Yahoo Data Breaches, even those made by persons who reside outside of California.  
15 In fact, California law should apply to all Plaintiffs’ claims, as the decisions and substandard acts on  
16 behalf of Defendants took place in California, and upon information and belief, the Plaintiffs’ PII  
17 was collected, stored on, and routed through California, and United States-based servers. For the  
18 sake of fairness and efficiency, California law should apply to these claims.

19 **CLAIMS ALLEGED ON BEHALF OF THE UNITED STATES CLASS, AND ISRAEL**

20 **CLASS**

21 **First Claim for Relief**

22 **Violation of California’s Unfair Competition Law (“UCL”)**

23 **(Cal. Bus. & Prof. Code § 17200, *et seq.*)**

24 126. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in  
25 paragraphs 1 through 125 as though fully stated herein.  
26

27 <sup>72</sup> *Id.*

28 <sup>73</sup> Centro de Privacidad de Yahoo, Yahoo!, <https://policies.yahoo.com/ie/es/yahoo/privacy/index.htm> (last visited Apr. 8, 2017).

1           127. By reason of the conduct alleged herein, Yahoo engaged in unlawful, unfair, and  
2 deceptive practices within the meaning of the UCL. The conduct alleged herein is a “business  
3 practice” within the meaning of the UCL.

4           128. Yahoo stored the PII of Plaintiffs and members of their respective classes in Yahoo’s  
5 electronic and consumer information databases. Yahoo represented to Plaintiffs and members of the  
6 classes that their PII databases were secure and that class members’ PII would remain private. Yahoo  
7 engaged in unfair acts and business practices by misleadingly providing on its website that  
8 “protecting our systems and our users’ information is paramount to ensuring Yahoo users enjoy a  
9 secure user experience and maintaining our users’ trust” and by representing that it had “physical,  
10 electronic, and procedural safeguards that comply with federal regulations to protect personal  
11 information about you.”<sup>74</sup>

12           129. Further, even without these representations, Plaintiffs and Class members were  
13 entitled to, and did, assume Yahoo would take appropriate measures to keep their PII safe. Yahoo  
14 did not disclose at any time that Plaintiffs’ PII was vulnerable to hackers because Yahoo’s data  
15 security measures were inadequate and outdated.

16           130. Yahoo knew or should have known it did not employ reasonable measures that would  
17 have kept Plaintiffs’ and the other Class members’ PII and financial information secure and  
18 prevented the loss or misuse of Plaintiffs’ and the other class members’ PII and financial  
19 information. Indeed, at the time of the 2013 Breach, Yahoo’s data encryption protocol, known as  
20 MD5, was widely discredited and had been proven, many years prior, easy to break. Additionally,  
21 Yahoo’s corporate culture discouraged expenditures that would make their data protection and  
22 encryption measures effective.

23           131. Yahoo’s representations that it would secure and protect the PII and financial  
24 information of Plaintiffs’ and members of the Classes were facts that reasonable persons could be  
25 expected to rely upon when deciding whether to use Yahoo’s services.

---

26  
27  
28 <sup>74</sup> Security at Yahoo, Yahoo!, <https://policies.yahoo.com/us/en/yahoo/privacy/topics/security/index.htm> (last visited Apr. 8, 2017).



1           132. Yahoo violated the UCL by misrepresenting, both by affirmative conduct and by  
2           omission, the safety of its many systems and services, specifically the security thereof, and its ability  
3           to safely store Plaintiffs' and Class members' PII. Yahoo also violated the UCL by failing to  
4           immediately notify Plaintiffs and the other Class members of the Yahoo Data Breaches. If Plaintiffs  
5           and the other Class members had been notified in an appropriate fashion, they could have taken  
6           precautions to safeguard their PII.

7           133. Yahoo also violated its commitment to maintain the confidentiality and security of the  
8           PII of Plaintiffs and their respective Classes, and failed to comply with its own policies and  
9           applicable laws, regulations, and industry standards relating to data security.

10          134. Yahoo's acts, omissions, and misrepresentations as alleged herein were unlawful and  
11          in violation of, *inter alia*, Cal. Civ. Code § 1750 *et seq.*, Cal. Civ. Code § 1798.80 *et seq.*, 18 U.S.C.  
12          § 2702, and also Cal. Bus. & Prof. Code § 22576 (as a result of Yahoo failing to comply with its  
13          own posted privacy policy).

14          135. Plaintiffs and the other Class members suffered injury in fact and lost money or  
15          property as the result of Yahoo's failure to secure Plaintiffs' and the other Class members' PII  
16          contained in Yahoo's servers or databases. In particular, Plaintiffs and Class members have suffered  
17          from forged credit applications and tax returns; improper or fraudulent charges to their credit/debit  
18          card accounts; hacked emails; and other similar harm, all as a result of the Yahoo Data Breaches. In  
19          addition, their PII was taken and is in the hands of those who will use it for their own advantage, or  
20          is being sold for value, making it clear that the hacked information is of tangible value. Plaintiffs and  
21          the Class members have also suffered consequential out of pocket losses for procuring credit freeze  
22          or protection services, identity theft monitoring, and other expenses relating to identity theft losses or  
23          protective measures.

24          136. As a result of Yahoo's violations of the UCL, Plaintiffs and the other Class members  
25          are entitled to restitution and injunctive relief.

**Second Claim for Relief**

**Violation of California's Consumer Legal Remedies Act ("CLRA")**

**(Cal. Civ. Code § 1750, *et seq.*)**

137. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 125 as though fully stated herein.

138. The CLRA was enacted to protect consumers against unfair and deceptive business practices. It extends to transactions that are intended to result, or which have resulted, in the sale of goods or services to consumers. Yahoo's acts, omissions, representations, and practices as described herein fall within the CLRA.

139. Plaintiffs and the other class members are consumers within the meaning of Cal. Civ. Code § 1761(d).

140. Yahoo's acts, omissions, misrepresentations, and practices were and are likely to deceive consumers. By misrepresenting the safety and security of its electronic and customer information databases, Yahoo violated the CLRA. Yahoo had exclusive knowledge of undisclosed material facts, namely, that its consumer databases were defective and/or unsecure, and withheld that knowledge from Plaintiffs and the other Class members. In addition, Yahoo had contemporaneous knowledge of the 2014 Data Breach and of the Forged Cookie Breach, which it failed to disclose, and withheld from Plaintiffs and the other Class members.

141. Yahoo's acts, omissions, misrepresentations, and practices alleged herein violated the following provisions of the CLRA, Civil Code § 1770, which provides, in relevant part, that:

(a) The following unfair methods of competition and unfair or deceptive acts or practices undertaken by any person in a transaction intended to result or which results in the sale or lease of goods or services to any consumer are unlawful:

(5) Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have ...

(7) Representing that goods or services are of a particular standard, quality, or grade . . . if they are of another.

1 (14) Representing that a transaction confers or involves rights,  
2 remedies, or obligations which it does not have or involve, or  
3 which are prohibited by law.

4 (16) Representing that the subject of a transaction has been  
5 supplied in accordance with a previous representation when it has  
6 not.

7 142. Yahoo stored Plaintiffs' and Class members' PII in its electronic and consumer  
8 information databases. Yahoo represented to Plaintiffs and the other Class members that its PII  
9 databases were secure and that customers' PII would remain private. Yahoo engaged in deceptive  
10 acts and business practices by providing in its website that "protecting our systems and our users'  
11 information is paramount to ensuring Yahoo users enjoy a secure user experience and maintaining  
12 our users' trust." Yahoo represented that it has "physical, electronic, and procedural safeguards that  
13 comply with federal regulations to protect personal information about you."<sup>75</sup>

14 143. Yahoo knew or should have known that it did not employ reasonable measures to  
15 keep Plaintiffs' and Class members' PII or financial information secure and prevent the loss or  
16 misuse of that information. In fact, Yahoo violated its commitment to maintain the confidentiality  
17 and security of the PII of Plaintiffs and the Class, and failed to comply with its own policies as well  
18 as applicable laws, regulations, and industry standards relating to data security.

19 144. Yahoo's deceptive acts and business practices induced Plaintiffs and the other Class  
20 members to use Yahoo's online services, and to provide their PII and financial information. But for  
21 these deceptive acts and business practices, Plaintiffs and the Class would not have provided that  
22 information to Yahoo.

23 145. Plaintiffs and the other Class members were harmed as the result of Yahoo's  
24 violations of the CLRA, because their PII and financial information were compromised, placing  
25 them at a greater risk of identity theft and of their PII and financial information being disclosed to  
26 third parties without their consent. Plaintiffs and Class members also suffered diminution in value of  
27 their PII in that it is now easily available to hackers on the Dark Web. Plaintiffs and the Class have

28 <sup>75</sup> See *supra* note 74.

1 also suffered consequential out of pocket losses for procuring credit freeze or protection services,  
 2 identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

3 146. Plaintiffs and the Class suffered injury in fact and lost money or property as the result  
 4 of Yahoo's failure to secure Plaintiffs' and the other Class members' PII and financial information.

5 147. As the result of Yahoo's violation of the CLRA, Plaintiffs and the Class are, or will  
 6 be, entitled to compensatory and exemplary damages, an order enjoining Yahoo from continuing the  
 7 unlawful practices described herein, a declaration that Yahoo's conduct violated the CLRA,  
 8 attorneys' fees, and the costs of litigation.

9 148. Pursuant to Civil Code § 1782, on September 30, 2016, in the case of *Myers, et al., v.*  
 10 *Yahoo! Inc.*, Case No. 16-cv-2391, filed in the Southern District of California and consolidated with  
 11 this action, Plaintiffs Paul Dugas and Rajesh Garg, on behalf of themselves and all others similarly  
 12 situated, notified Yahoo in writing by certified mail of the alleged violations of section 1770 and  
 13 demanded that the same be corrected. In an abundance of caution, all named Plaintiffs in this  
 14 Consolidated Class Action Complaint are serving an additional notice under section 1782  
 15 concurrently with the filing of this Complaint.

16 **CLAIMS ALLEGED ON BEHALF OF THE UNITED STATES CLASS, SMALL BUSINESS**

17 **USERS' CLASS, AND ISRAEL CLASS**

18 **Third Claim for Relief**

19 **Violation of California's Data Breach Notification Law**

20 **(Cal. Civ. Code § 1798.80, *et seq.*)**

21 149. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in  
 22 paragraphs 1 through 125 as though fully stated herein.

23 150. Section 1798.82 of the California Civil Code provides, in pertinent part:

24 (a) Any person or business that conducts business in California, and that  
 25 owns or licenses computerized data that includes personal information,  
 26 shall disclose any breach of the security of the system following discovery  
 27 or notification of the breach in the security of the data to any resident of  
 28 California whose unencrypted personal information was, or is reasonably  
 believed to have been, acquired by an unauthorized person. The disclosure  
 shall be made in the most expedient time possible and without

1 unreasonable delay, consistent with the legitimate needs of law  
 2 enforcement, as provided in subdivision (c), or any measures necessary to  
 3 determine the scope of the breach and restore the reasonable integrity of  
 4 the data system.

5 (b) Any person or business that maintains computerized data that includes  
 6 personal information that the person or business does not own shall notify  
 7 the owner or licensee of the information of any breach of the security of  
 8 the data immediately following discovery, if the personal information was,  
 9 or is reasonably believed to have been, acquired by an unauthorized  
 10 person.

11 (c) The notification required by this section may be delayed if a law  
 12 enforcement agency determines that the notification will impede a  
 13 criminal investigation. The notification required by this section shall be  
 14 made after the law enforcement agency determines that it will not  
 15 compromise the investigation.

16 (d) Any person or business that is required to issue a security breach  
 17 notification pursuant to this section shall meet all of the following  
 18 requirements:

19 (1) The security breach notification shall be written in plain language.

20 (2) The security breach notification shall include, at a minimum, the  
 21 following information:

22 (A) The name and contact information of the reporting person or  
 23 business subject to this section.

24 (B) A list of the types of personal information that were or are  
 25 reasonably believed to have been the subject of a breach.

26 (C) If the information is possible to determine at the time the  
 27 notice is provided, then any of the following: (i) the date of the  
 28 breach, (ii) the estimated date of the breach, or (iii) the date range  
 within which the breach occurred. The notification shall also  
 include the date of the notice.

(D) Whether notification was delayed as a result of a law  
 enforcement investigation, if that information is possible to  
 determine at the time the notice is provided.

(E) A general description of the breach incident, if that information  
 is possible to determine at the time the notice is provided.

1 (F) The toll-free telephone numbers and addresses of the major  
2 credit reporting agencies if the breach exposed a social security  
3 number or a driver's license or California identification card  
4 number.

5 151. The Yahoo Data Breaches described previously in this Complaint each constituted a  
6 "breach of the security system" of Yahoo and Aabaco.

7 152. As alleged above, Defendants Yahoo and Aabaco unreasonably delayed informing  
8 anyone about the 2013 Breach, the 2014 Breach, and the Forged Cookies Breach, affecting  
9 Plaintiffs' and other Class members' confidential and non-public PII and financial information after  
10 Defendants knew each of the Yahoo Data Breaches had occurred.

11 153. Defendants Yahoo and Aabaco failed to disclose to Plaintiffs and the Class members,  
12 without unreasonable delay and in the most expedient time possible, the breach of security of their  
13 unencrypted, or not properly and securely encrypted, PII and financial information when Defendants  
14 Yahoo and Aabaco knew or reasonably believed such information had been compromised.

15 154. Yahoo's ongoing business interests, and in particular its impending sale to Verizon,  
16 gave Yahoo incentive to conceal the Yahoo Data Breaches from the public to ensure continued  
17 revenue and a high stock price for the sale.

18 155. Upon information and belief, no law enforcement agency instructed Defendants  
19 Yahoo and Aabaco that notification to Plaintiffs or other Class members would impede its  
20 investigation.

21 156. Pursuant to Section 1798.84 of the California Civil Code:

22 (a) Any waiver of a provision of this title is contrary to public policy and  
23 is void and unenforceable.

24 (b) Any customer injured by a violation of this title may institute a civil  
25 action to recover damages.(c) In addition, for a willful, intentional, or  
26 reckless violation of Section 1798.83, a customer may recover a civil  
27 penalty not to exceed three thousand dollars (\$3,000) per violation;  
28 otherwise, the customer may recover a civil penalty of up to five hundred  
dollars (\$500) per violation for a violation of Section 1798.83.

\* \* \* \* \*



(e) Any business that violates, proposes to violate, or has violated this title may be enjoined.

157. As a result of Defendants Yahoo and Aabaco's violation of Cal. Civ. Code § 1798.82, Plaintiffs' and the Class members' PII and financial information were compromised, placing them at a greater risk of identity theft and their PII and financial information disclosed to third parties without their consent. Plaintiffs and Class members also suffered diminution in value of their PII in that it is now easily available to hackers on the Dark Web. Plaintiffs and the Class have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures. The Class members are further damaged as their PII remains in Defendants' possession, without adequate protection, and is also in the hands of those who obtained it without their consent.

158. Plaintiffs, on behalf of themselves and members of their respective classes, seek all remedies available under Cal. Civ. Code § 1798.84, including, but not limited to: (a) damages suffered by Plaintiffs and the other class members as alleged above; (b) statutory penalties of up to \$3,000 per violation for Defendants Yahoo and Aabaco's willful, intentional, and/or reckless violations of Cal. Civ. Code § 1798.83 (or, at a minimum, up to \$500 per violation); and (c) equitable relief.

159. Plaintiffs and the Class also seek reasonable attorneys' fees and costs under Cal. Civ. Code § 1798.84(g).

#### **Fourth Claim for Relief**

#### **Violation of Stored Communications Act**

#### **(18 U.S.C. § 2702)**

160. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 125 as though fully stated herein.

161. The Federal Stored Communications Act ("SCA") contains provisions that provide customers of entities providing electronic communication services to the public with redress if a company mishandles their electronically stored information.

1           162. Section 2702(a)(1) of the SCA provides that “a person or entity providing an  
2 electronic communication service to the public shall not knowingly divulge to any person or entity  
3 the contents of a communication while in electronic storage by that service.” 18 U.S.C. § 2702(a)(1).

4           163. The SCA defines “electronic communication service” as “any service which provides  
5 to users thereof the ability to send or receive wire or electronic communications.” *Id.* § 2510(15).

6           164. Through their equipment, Defendants Yahoo and Aabaco provide an “electronic  
7 communication service to the public” within the meaning of the SCA because they provide  
8 consumers at large with mechanisms that enable them to send or receive wire or electronic  
9 communications concerning all facets of their lives, including PII.

10           165. By failing to take commercially reasonable steps to safeguard the PII and sensitive  
11 financial information of Plaintiffs and the class members, even after Defendants Yahoo and Aabaco  
12 were aware that their PII had been compromised, Defendants Yahoo and Aabaco knowingly  
13 divulged the PII and sensitive financial information of Plaintiffs and the class members while in  
14 electronic storage in Defendants’ system.

15           166. Section 2702(a)(2)(A) of the SCA provides that “a person or entity providing remote  
16 computing service to the public shall not knowingly divulge to any person or entity the contents of  
17 any communication which is carried or maintained on that service on behalf of, and received by  
18 means of electronic transmission from (or created by means of computer processing of  
19 communications received by means of electronic transmission from), a subscriber or customer of  
20 such service.” 18 U.S.C. § 2702(a)(2)(A).

21           167. The SCA defines “remote computing service” as “the provision to the public of  
22 computer storage or processing services by means of an electronic communication system.” 18  
23 U.S.C. § 2711(2).

24           168. An “electronic communications systems” is defined by the SCA as “any wire, radio,  
25 electromagnetic, photo-optical or photo-electronic facilities for the transmission of wire or electronic  
26 communications, and any computer facilities or related electronic equipment for the electronic  
27 storage of such communications.” 18 U.S.C. § 2510(4).

169. Defendants Yahoo and Aabaco provide remote computing services to the public by virtue of their computer processing services for electronic communications. These services are used by Defendants' customers and carried out by means of an electronic communications system, namely the use of wire, electromagnetic, photo-optical or photo-electric facilities for the transmission of wire or electronic communications received from, and on behalf of, the customer.

170. By failing to take commercially reasonable steps to safeguard PII, even after Defendants Yahoo and Aabaco were aware that customers' PII and private financial information had been compromised, Defendants Yahoo and Aabaco knowingly divulged the PII and private financial information carried and maintained on Defendants' remote computing service.

171. As a result of Defendants Yahoo and Aabaco's conduct and their violations of Section 2702(a)(1) and (2)(A), Plaintiffs and the Class members have suffered injuries, including various forms of identity theft and lost money and the costs associated with the need for vigilant credit monitoring to protect against additional identity theft. Plaintiffs, on their own behalf and on behalf of the putative classes, seek an order awarding themselves and the class members the maximum statutory damages available under 18 U.S.C. § 2707, in addition to the cost for 3 years of credit monitoring services.

### **Fifth Claim for Relief**

#### **Violation of California's Online Privacy Protection Act**

#### **(Cal. Bus. & Prof. Code § 22575, *et seq.*)**

172. Plaintiffs, repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 125 as though fully stated herein.

173. Yahoo is a commercial website or online service that collects personally identifiable information through the Internet about individual consumers residing in California, and elsewhere, who use or visit its commercial Web site or online services, within the meaning of California Business and Professions Code § 22575(a).

174. Aabaco is also a commercial website or online service that collects personally identifiable information through the Internet about individual consumers residing in California, and

1 elsewhere, who use or visit its commercial website or online services, within the meaning of  
2 California Business and Professions Code § 22575(a).

3 175. Defendants Yahoo and Aabaco failed to adhere to their posted privacy policy  
4 concerning the care they would take to safeguard Plaintiffs' and Class members' PII, and negligently  
5 and materially failed to adhere to their posted privacy policy with respect to the extent of their  
6 disclosure of users' data, in violation of California Business and Professions Code § 22576.

7 176. As a result of Defendants' failures to adhere to their privacy policies and their  
8 violations of California Business and Professions Code § 22575, *et seq.*, Plaintiffs and the Class have  
9 suffered injuries described in detail herein. Plaintiffs, on their own behalf and on behalf of the  
10 putative classes, seek all remedies available under California Business and Professions Code  
11 § 22575, *et seq.*

12 **CLAIMS ALLEGED ON BEHALF OF THE UNITED STATES CLASS, SMALL BUSINESS**

13 **USERS CLASS, AND ISRAEL CLASS**

14 **Sixth Claim for Relief**

15 **Breach of Contract**

16 177. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in  
17 paragraphs 1 through 125 as though fully stated herein.

18 178. Yahoo's Privacy Policy is incorporated by reference into its Terms of Service, which  
19 forms a binding contract between Yahoo and each user at the time of the creation of an account.  
20 Yahoo's Terms of Service for 2011-2016 are attached to this Complaint as Exhibit 1.

21 179. Yahoo breached the contract with respect to at least the following four provisions of  
22 the Privacy Policy.

23 a. "We are committed to ensuring your information is protected and apply  
24 safeguards in accordance with applicable law."

25 b. "Yahoo does not rent, sell, or share personal information about you with other  
26 people or non-affiliated companies except to provide products or services you've requested,  
27 when we have your permission, or under [certain inapplicable circumstances]."  
28

1 c. “We limit access to personal information about you to employees who we  
2 reasonably believe need to come into contact with that information to provide products or  
3 services to you or in order to do their jobs.”

4 d. “We have physical, electronic, and procedural safeguards that comply with  
5 federal regulations to protect personal information about you.”

6 180. Aabaco’s Privacy Policy is similarly incorporated by reference into its Terms of  
7 Service, forming a binding contract between Aabaco and each user at the time of purchasing any  
8 service or product from Aabaco. Aabaco’s Terms of Service for 2009 and 2011-2016 are attached to  
9 this Complaint as Exhibit 2. Aabaco’s Privacy Policy further provides that Aabaco shares PII with  
10 Yahoo, and “Yahoo’s Privacy Policy governs its use of that information.”

11 181. Aabaco breached the contract with respect to at least the following three provisions of  
12 its Privacy Policy:

13 a. “The Company does not rent, sell, or share Personal Information about You  
14 with other people or non-affiliated companies except to provide products or services You’ve  
15 requested, when we have Your permission, or under the following circumstances: ...”

16 b. “We limit access to Personal Information about You to employees,  
17 contractors, or service providers who we believe reasonably need to come into contact with  
18 that information to provide products or services to You or in order to do their jobs.”

19 c. “We have physical, electronic, and procedural safeguards that comply with  
20 federal regulations to protect Personal Information about You.”

21 182. Defendants Yahoo and Aabaco breached these provisions of the contracts in that they  
22 did not have proper safeguards “in accordance with applicable law” to protect Plaintiffs’ and Class  
23 members’ “Personal Information,” and did not limit access to that information to the specified  
24 individuals or entities. Defendants Yahoo and Aabaco violated their commitment to maintain the  
25 confidentiality and security of the PII of Plaintiffs and the class members, and failed to comply with  
26 their own policies and applicable laws, regulations, and industry standards relating to data security.

27 183. The 2013, 2014, and Forged Cookie Data Breaches were a direct and legal cause of  
28 the injuries and damages suffered by Plaintiffs and the Class members.

184. Plaintiffs and the other Class members were harmed as the result of the 2013, 2014, and Forged Cookie Data Breaches because their PII and financial information were compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their PII and financial information was disclosed to third parties without their consent. Plaintiffs and Class members also suffered diminution in value of their PII in that it is now easily available to hackers on the Dark Web. In addition, Plaintiff Neff and the members of the Small Business Users Class were damaged to the extent of all or part of the amounts they paid for small business services, because those services were either worth nothing or worth less than was paid for them because of their lack of security. Plaintiffs and the Class have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

#### **Seventh Claim for Relief**

##### **Breach of Implied Contracts**

185. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 125 as though fully stated herein.

186. To the extent that Defendants' Terms of Service and Privacy Policies did not form express contracts, the opening of a Yahoo or Aabaco account created implied contracts between Defendants and the user, the terms of which were set forth by the relevant Terms of Service and Privacy Policy.

187. Defendants Yahoo and Aabaco breached such implied contracts by failing to adhere to the terms of the applicable Policy, as described above. Defendants Yahoo and Aabaco violated their commitment to maintain the confidentiality and security of the PII of Plaintiffs and the Class, and failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security.

188. Plaintiffs and the Class members were harmed as the result of Defendants Yahoo and Aabaco's breach of the implied contracts because their PII and financial information were compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their PII and financial information was disclosed to third parties without their consent. Plaintiffs



1 and Class members also suffered diminution in value of their PII in that it is now easily available to  
 2 hackers on the Dark Web. In addition, Plaintiff Neff and the members of the Small Business Users  
 3 Class were damaged to the extent of all or part of the amounts they paid for small business services,  
 4 because those services were either worth nothing or worth less than was paid for them because of  
 5 their lack of security. Plaintiffs and the Class have also suffered consequential out of pocket losses  
 6 for procuring credit freeze or protection services, identity theft monitoring, and other expenses  
 7 relating to identity theft losses or protective measures. The Class members are further damaged as  
 8 their PII remains in Defendants' possession, without adequate protection, and is also in the hands of  
 9 those who obtained it without their consent.

10 189. This breach of the implied contracts was a direct and legal cause of the injuries and  
 11 damages to Plaintiffs and members of the Class as described above.

### 12 **Eighth Claim for Relief**

#### 13 **Breach of the Implied Covenant of Good Faith and Fair Dealing**

14 190. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in  
 15 paragraphs 1 through 125 as though fully stated herein.

16 191. Under California law there is an implied covenant of good faith and fair dealing in  
 17 every contract that neither party will do anything which will injure the right of the other to receive  
 18 the benefits of the agreement.

19 192. Under the express and implied terms of the agreements entered into between  
 20 Defendants Yahoo and Aabaco and Plaintiffs and the Class members, Plaintiffs and the Class  
 21 members were to benefit through the use of Defendants Yahoo and Aabaco's services, while those  
 22 Defendants were supposed to benefit through the limited use of users' data for advertising and  
 23 product enhancement purposes.

24 193. Defendants Yahoo and Aabaco exhibited bad faith through their conscious awareness  
 25 of and deliberate indifference to the risks to Class members' PII, including by (a) using password  
 26 encryption standards that were long known to be unsafe; (b) taking no serious action in response to  
 27 past breaches; (c) falling well behind industry standards of cybersecurity; and (d) under-investing in  
 28

1 cybersecurity resources despite assurances to its users to the contrary. In doing so, Defendants  
2 Yahoo and Aabaco acted well outside of commercially reasonable norms.

3 194. Defendants Yahoo and Aabaco, by exposing their users to vastly greater and more  
4 harmful exploitation of their PII than they had bargained for, breached the implied covenant of good  
5 faith and fair dealing with respect to both the specific contractual terms in Yahoo's Privacy Policy  
6 and Aabaco's Privacy Policy and the implied warranties of their contractual relationships with their  
7 users.

8 195. Plaintiffs and the other Class members were harmed as the result of Defendants  
9 Yahoo and Aabaco's breach of the implied covenant of good faith and fair dealing because their PII  
10 and financial information were compromised, placing them at a greater risk of identity theft and their  
11 PII and financial information disclosed to third parties without their consent. Plaintiffs and Class  
12 members also suffered diminution in value of their PII in that it is now easily available to hackers on  
13 the Dark Web. Plaintiff Neff and the members of the Small Business Users Class were damaged to  
14 the extent of all or part of the amounts they paid for small business services, because those services  
15 were either worth nothing or worth less than was paid for them because of their lack of security.  
16 Plaintiffs and the Class have also suffered consequential out of pocket losses for procuring credit  
17 freeze or protection services, identity theft monitoring, and other expenses relating to identity theft  
18 losses or protective measures. The Class members are further damaged as their PII remains  
19 Defendants' possession, without adequate protection, and is also in the hands of those who obtained  
20 it without their consent.

21  
22 **CLAIMS ALLEGED ON BEHALF OF THE SMALL BUSINESS USERS CLASS**

23 **Ninth Claim for Relief**

24 **Fraudulent Inducement**

25 196. Plaintiff Neff repeats, realleges, and incorporates by reference the allegations  
26 contained in paragraphs 1 through 125 as though fully stated herein.

27 197. Since November 2015, Aabaco, a wholly owned and controlled subsidiary of Yahoo  
28 has been the business entity that Yahoo uses to provide services to small business owners. Aabaco is

1 the successor in interest to the Yahoo Small Business division and is liable as the successor for any  
2 wrongdoing by that division before it was dissolved by Yahoo and re-named Aabaco. At all times  
3 herein relevant since November 2015, Aabaco has been the alter ego of Yahoo for its small business  
4 services.

5 198. Yahoo and Aabaco made numerous representations, in advertising and in the Privacy  
6 Policy, regarding the supposed secure nature of their small business services. Such representations  
7 were false because Yahoo and Aabaco utilized outdated encryption protocols, and failed to disclose  
8 that they did not use reasonable, industry-standard means, to safeguard against hacking and theft of  
9 customer PII.

10 199. Such representations were material to customers and would-be customers, who  
11 reasonably relied on the representations. Plaintiff Neff and other Small Business Users Class  
12 members would not have agreed to utilize and pay for the small business services and turn over PII,  
13 had they known the truth: that the services of Yahoo and Aabaco were not as secure as represented  
14 or secure by any standard.

15 200. Yahoo and Aabaco intended for Plaintiff Neff and other Class members to rely on  
16 their security representations, as they knew no would-be customer would submit PII or entrust an  
17 online business to unreasonable security risks.

18 201. Yahoo and Aabaco's representations were made with knowledge of their falsity, or at  
19 least with extreme disregard for their truth.

20 202. Yahoo had experienced several data breaches prior to the 2013 Breach (and after),  
21 had been warned that its encryption was outdated, and rejected the advice from its own security  
22 employees or contractors to improve security. This knowledge is imputed to Aabaco as a wholly  
23 owned and controlled subsidiary and alter ego of Yahoo.

24 203. As a direct and proximate result of Yahoo and Aabaco's wrongful action and  
25 inaction, Plaintiff Neff and the other Small Business Users Class members have been damaged by  
26 paying monthly fees to Yahoo and Aabaco for something they did not receive: secure small business  
27 services. Plaintiff Neff and the other Small Business Users Class members were also damaged by  
28 experiencing actual identity theft (as in Plaintiff Neff's case) and/or placed at an imminent,

1 immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring  
 2 them to take the time and effort to mitigate the actual and potential impact of the Yahoo Data  
 3 Breaches on their lives.

4 **Tenth Claim for Relief**

5 **Negligent Misrepresentation**

6 **(In The Alternative to The Claim For Fraudulent Inducement)**

7 204. Plaintiff Neff repeats, realleges, and incorporates by reference the allegations  
 8 contained in paragraphs 1 through 125 as though fully stated herein.

9 205. Defendants Yahoo and Aabaco made numerous representations, in their advertising  
 10 and in their Privacy Policies, regarding the supposed secure nature of their small business services.  
 11 Such representations were false because Defendants Yahoo and Aabaco utilized outdated encryption,  
 12 and failed to disclose that they did not use reasonable, industry-standard means, to safeguard against  
 13 hacking and theft of customer PII.

14 206. Such representations were material to customers and would-be customers, who  
 15 reasonably relied on the representations. Plaintiff Neff and other members of the Small Business  
 16 Users Class would not have agreed to utilize and pay for the small business services and turn over  
 17 PII, had they known the truth: that Defendants Yahoo and Aabaco's services were not as secure as  
 18 represented or secure by any standard.

19 207. Defendants Yahoo and Aabaco intended that Plaintiff Neff and other Small Business  
 20 Users Class members rely on their security representations, as they knew no would-be customer  
 21 would submit PII or entrust an online business to unreasonable security risks. In reliance on these  
 22 representations and omissions, Plaintiff and the Small Business Users Class contracted with Yahoo  
 23 and Aabaco for email and web services, and provided their PII, which was ancillary to, but not the  
 24 subject of, the contracts for services. In addition, Plaintiff Neff and other Small Business Users Class  
 25 members used Yahoo's and Aabaco's email and web services to complete transactions or send  
 26 sensitive information including PII. This provision of PII was not part of the contracts with Yahoo  
 27 and Aabaco.  
 28

208. Defendants Yahoo and Aabaco experienced several data breaches prior to the 2013 Breach (and after), had been warned that their encryption was outdated, and rejected the advice from their own security employees or contractors to improve security. Defendants were negligent in their representations.

209. As a direct and proximate result of Defendants Yahoo and Aabaco's wrongful actions and inactions, Plaintiff Neff and the other Small Business Users Class members have been damaged by paying monthly fees to Defendants Yahoo and Aabaco for something they did not receive: secure small business services.

210. As a direct and proximate result of Defendants' negligent, and/or willful, actions and inactions, Plaintiff Neff and the other Small Business Users Class members experienced damage to the PII supplied to Defendants for purposes of their business services contracts, actual identity theft (as in Plaintiff Neff's case) and/or being placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time and effort to mitigate the actual and potential impact of the Yahoo Data Breaches on their lives.

211. As a direct and proximate result of Defendants Yahoo and Aabaco's negligent, and/or willful, actions and inactions, Plaintiff Neff and the other Small Business Users Class members experienced damage to property that was not the subject of the business services contracts with Defendants Yahoo and Aabaco, including but not limited to the PII contained within private email communications, actual identity theft (as in Plaintiff Neff's case), damage to their credit, damage to their businesses, and/or being placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time and effort to mitigate the actual and potential impact of the Yahoo Data Breaches on their lives.

### **Eleventh Claim for Relief**

#### **Violation of California's Unfair Competition Law ("UCL")**

**(Cal. Bus. & Prof. Code § 17200, *et seq.*)**

212. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 125 as though fully stated herein.

1           213. Since November 2015, Aabaco, a wholly owned and controlled subsidiary of Yahoo  
2 has been the business entity that Yahoo uses to provide services to small business owners. Aabaco is  
3 the successor in interest to the Yahoo Small Business division and is liable as the successor for any  
4 wrongdoing by that division before it was dissolved by Yahoo and re-named Aabaco. At all times  
5 herein relevant since November 2015, Aabaco has been the alter ego of Yahoo for its small business  
6 services.

7           214. By reason of the conduct alleged herein, Yahoo and Aabaco engaged in unlawful,  
8 unfair, and deceptive practices within the meaning of the UCL. The conduct alleged herein is a  
9 “business practice” within the meaning of the UCL.

10           215. Yahoo and Aabaco stored the PII of Plaintiffs and members of their respective classes  
11 in Yahoo and/or Aabaco’s electronic and consumer information databases. Yahoo and Aabaco  
12 represented to Plaintiffs and members of the classes that their PII databases were secure and that  
13 class members’ PII would remain private. Yahoo and Aabaco engaged in unfair acts and business  
14 practices by misleadingly providing on their website that “protecting our systems and our users’  
15 information is paramount to ensuring Yahoo and Aabaco users enjoy a secure user experience and  
16 maintaining our users’ trust” and by representing that they had “physical, electronic, and procedural  
17 safeguards that comply with federal regulations to protect personal information about you.”<sup>76</sup>

18           216. Further, even without these representations, Plaintiffs and Class members were  
19 entitled to, and did, assume Yahoo and Aabaco would take appropriate measures to keep their PII  
20 safe. Yahoo and Aabaco did not disclose at any time that Plaintiffs’ PII was vulnerable to hackers  
21 because Yahoo and Aabaco’s data security measures were inadequate and outdated.

22           217. Yahoo and Aabaco knew or should have known they did not employ reasonable  
23 measures that would have kept Plaintiffs’ and the other Class members’ PII and financial  
24 information secure and prevented the loss or misuse of Plaintiffs’ and the other class members’ PII  
25 and financial information. Indeed, at the time of the 2013 Breach, Yahoo’s data encryption protocol,  
26 known as MD5, was widely discredited and had been proven, many years prior, easy to break.

27 \_\_\_\_\_  
28 <sup>76</sup> See *supra* note 74.

1 Additionally, Yahoo and Aabaco's corporate culture discouraged expenditures that would make their  
2 data protection and encryption measures effective.

3 218. Yahoo and Aabaco's representations that they would secure and protect the PII and  
4 financial information of Plaintiffs' and members of the classes were facts that reasonable persons  
5 could be expected to rely upon when deciding whether to use Yahoo and Aabaco's services.

6 219. Yahoo and Aabaco violated the UCL by misrepresenting, both by affirmative conduct  
7 and by omission, the safety of their many systems and services, specifically the security thereof, and  
8 their ability to safely store Plaintiffs' and Class members' PII. Yahoo and Aabaco also violated the  
9 UCL by failing to immediately notify Plaintiffs and the other Class members of the Yahoo Data  
10 Breaches. If Plaintiffs and the other Class members had been notified in an appropriate fashion, they  
11 could have taken precautions to safeguard their PII.

12 220. Yahoo and Aabaco also violated their commitment to maintain the confidentiality and  
13 security of the PII of Plaintiffs and their respective Classes, and failed to comply with their own  
14 policies and applicable laws, regulations, and industry standards relating to data security.

15 221. Yahoo and Aabaco's acts, omissions, and misrepresentations as alleged herein were  
16 unlawful and in violation of, inter alia, Cal. Civ. Code § 1750 *et seq.*, Cal. Civ. Code § 1798.80 *et*  
17 *seq.*, 18 U.S.C. § 2702, and also Cal. Bus. & Prof. Code § 22576 (as a result of Yahoo and Aabaco  
18 failing to comply with their own posted privacy policy).

19 222. Plaintiffs and the other Class members suffered injury in fact and lost money or  
20 property as the result of Yahoo and Aabaco's failure to secure Plaintiffs' and the other Class  
21 members' PII contained in Yahoo and/or Aabaco's servers or databases. In particular, Plaintiffs and  
22 Class members have suffered from forged credit applications and tax returns; improper or fraudulent  
23 charges to their credit/debit card accounts; hacked emails; and other similar harm, all as a result of  
24 the Yahoo Data Breaches. In addition, their PII was taken and is in the hands of those who will use it  
25 for their own advantage, or is being sold for value, making it clear that the hacked information is of  
26 tangible value. Plaintiffs and the Class members have also suffered consequential out of pocket  
27 losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses  
28 relating to identity theft losses or protective measures.



223. As a result of Yahoo and Aabaco's violations of the UCL, Plaintiffs and the other Class members are entitled to restitution and injunctive relief.

**CLAIM ALLEGED ON BEHALF OF THE AUSTRALIA, VENEZUELA, AND SPAIN**

**CLASS**

**Twelfth Claim for Relief**

**Negligence**

224. Plaintiffs Corso, Abitol, and Robles repeat, reallege, and incorporate by reference the allegations contained in paragraph 1 through 125 as though fully stated herein.

225. Yahoo owed a duty to the Plaintiffs Corso, Abitol, and Robles and the members of the Australia, Venezuela, and Spain Class to exercise reasonable care in safeguarding and protecting the Australia, Venezuela, and Spain Class Members' PII and financial information in Yahoo's possession from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties. This duty included, among other things, designing, maintaining, and testing Defendants' security systems to ensure that Plaintiffs Corso, Abitol, and Robles's and the Australia, Venezuela, and Spain Class members' PII and financial information were adequately secured and protected. Yahoo further had a duty to implement processes that would detect a breach of its security system in a timely manner.

226. Yahoo also had a duty to timely disclose to Plaintiffs Corso, Abitol, and Robles and the Australia, Venezuela, and Spain Class that their PII and financial information had been, or was reasonably believed to have been, compromised. Timely disclosure was necessary so that, among other things, Plaintiffs Corso, Abitol, and Robles and the Australia, Venezuela, and Spain Class members could take appropriate measures to cancel or change usernames, PIN numbers, and passwords on compromised accounts, to begin monitoring their accounts for unauthorized access, to contact the credit bureaus to request freezes or place alerts, and take any and all other appropriate precautions.

227. Yahoo breached its duty to exercise reasonable care in safeguarding and protecting the PII and financial information of Plaintiffs Corso, Abitol, and Robles and the Australia,

1 Venezuela, and Spain Class by failing to adopt, implement, and maintain adequate security measures  
2 to safeguard that information; allowing unauthorized access to the PII and financial information of  
3 Plaintiffs Corso, Abitbol, and Robles and the Australia, Venezuela, and Spain Class members stored  
4 by Yahoo; and failing to recognize in a timely manner the Yahoo Data Breaches.

5 228. Yahoo breached its duty to timely disclose that the PII and financial information of  
6 Plaintiffs Corso, Abitbol, and Robles and the Australia, Venezuela, and Spain Class members had  
7 been, or was reasonably believed to have been, stolen or compromised.

8 229. Yahoo's failure to comply with industry regulations and the delay between the date of  
9 the breaches and the date Yahoo informed customers of the data breach further evidence Yahoo's  
10 negligence in failing to exercise reasonable care in safeguarding and protecting the PII and financial  
11 information of Plaintiffs Corso, Abitbol, and Robles and the Australia, Venezuela, and Spain Class  
12 members.

13 230. But for Yahoo's wrongful and negligent breach of its duties owed to Plaintiffs Corso,  
14 Abitbol, and Robles and the Australia, Venezuela, and Spain Class members, their PII and financial  
15 information would not have been compromised, stolen, and viewed by unauthorized persons.

16 231. The injury and harm suffered by Plaintiffs Corso, Abitbol, and Robles and the  
17 Australia, Venezuela, and Spain Class members was the reasonably foreseeable result of Yahoo's  
18 failure to exercise reasonable care in safeguarding and protecting the PII and financial information of  
19 Plaintiffs Corso, Abitbol, and Robles and the Australia, Venezuela, and Spain Class members.  
20 Yahoo knew or should have known that its systems and technologies for processing and securing the  
21 PII and financial information of Plaintiffs Corso, Abitbol, and Robles and the Australia, Venezuela,  
22 and Spain Class members had security vulnerabilities.

23 232. As a result of Yahoo's negligence, Plaintiffs Corso, Abitbol, and Robles and the  
24 Australia, Venezuela, and Spain Class members have incurred damages, including, *inter alia*,  
25 expenses for credit monitoring, fraudulent charges on credit card or bank accounts, forged IRS  
26 returns, loss of use and value of their debit and/or credit cards, and/or other identity or PII theft-  
27 related damages.

**CLAIMS FOR RELIEF MADE ON BEHALF OF ALL CLASSES**

**Thirteenth Claim for Relief**

**Declaratory Relief**

233. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 125 as though fully stated herein.

234. In connection with the active case and controversy between Plaintiffs and Defendants, Plaintiffs seek declaratory relief pursuant to 28 U.S.C. § 2201, declaring that:

a. To the extent Plaintiffs' claims for express or implied warranties are covered by Yahoo's Terms of Service, the disclaimer of warranties contained in § 19.1 is unconscionable and unenforceable;

b. To the extent Plaintiffs' claims are covered by Yahoo's Terms of Service, the limitation of liability in § 20 "resulting from...unauthorized access to ...[users'] data" is unconscionable and unenforceable, or precluded by federal and state law as recognized in § 21.

c. To the extent any Plaintiffs' claims for express or implied warranties are covered by Aabaco's Terms of Service, the disclaimer of warranties contained in § 12 is unconscionable and unenforceable;

d. To the extent Plaintiffs' claims are covered by Aabaco's Terms of Service, the limitation of liability in § 13 is unconscionable and unenforceable, or precluded by federal and state law; and

e. To the extent Plaintiffs' claims are covered by Aabaco's Terms of Service, the one-year limitation contained in § 20 is unconscionable and unenforceable.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiffs, individually and on behalf of the other Class members, respectfully requests that this Court enter an Order:

(a) Certifying the United States Class, Small Business Users' Class, Israel Class, Venezuela, Australia and Spain Class, and appointing Plaintiffs as Class Representatives;

(b) Finding that Defendants' conduct was negligent, deceptive, unfair, and unlawful as alleged herein;

(c) Enjoining Defendants from engaging in further negligent, deceptive, unfair, and unlawful business practices alleged herein;

(d) Awarding Plaintiffs and the Class members actual, compensatory, and consequential damages;

(e) Awarding Plaintiffs and the Class members statutory damages and penalties, as allowed by law;

(f) Awarding Plaintiffs and the Class members restitution and disgorgement;

(g) Requiring Defendants to provide appropriate credit monitoring services to Plaintiffs and the other class members;

(h) Awarding Plaintiffs and the Class members pre-judgment and post-judgment interest;

(i) Awarding Plaintiffs and the Class members reasonable attorneys' fees costs and expenses, and;

(j) Granting such other relief as the Court deems just and proper.

**JURY TRIAL DEMANDED**

Plaintiffs demand a trial by jury of all claims in this Consolidated Amended Class Action Complaint so triable.

Dated: April 12, 2017

CASEY GERRY SCHENK FRANCAVILLA  
BLATT & PENFIELD LLP

/s/ Gayle M. Blatt  
GAYLE M. BLATT

*Attorney for Plaintiffs*

On behalf of Plaintiffs' Lead Counsel and  
Executive Committee