Daniel S. Robinson (SBN 244245)
Wesley K. Polischuk (SBN 254121)
ROBINSON CALCAGNIE, INC.
19 Corporate Plaza Drive
Newport Beach, CA 92660
(949) 720-1288; Fax (949) 720-1292
drobinson@robinsonfirm.com
wpolischuk@robinsonfirm.com

JCCP Co-Lead Counsel for Plaintiffs

Brian D. Chase (SBN 164109)
Jerusalem F. Beligan (SBN 211258)
BISNAR | CHASE LLP
1301 Dove Street, Suite 120
Newport Beach, CA 92626
Tel.: (949) 752-2999; Fax: (949) 752-2777
bchase@bisnarchase.com
jbeligan@bisnarchase.com

JCCP Co-Lead Counsel for Plaintiffs

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF ORANGE

COORDINATION PROCEEDING SPECIAL TITLE [RULE 3.550] **YAHOO! INC. PRIVATE INFORMATION DISCLOSURE CASES**	JUDICIAL COUNCIL COORDINATION PROCEEDING NO. 4895 Assigned for All Purposes to: Hon. Thierry P. Colaw; Dept. CX105 **CONSOLIDATED CLASS ACTION COMPLAINT**
THIS DOCUMENT RELATES TO: *All Cases*	**JURY TRIAL DEMAND**

Plaintiffs Jared Pastor, Brendan Quinn, John Bell, Hilary Gamache, Jana Brabcova, Michelle Bouras, and Reid Bracken ("Plaintiffs"), by their undersigned attorneys, on behalf of themselves and all other California citizens similarly situated (the "Class" or "Class members"), bring this Consolidated Class Action Complaint ("Complaint") against Defendant Yahoo! Inc. and Does 1-100 (collectively, "Yahoo" or "Defendant"), with personal knowledge as to their own actions, and upon information and belief as to those of others, and respectfully allege the following:

NATURE OF THE ACTION

1. This class action seeks to redress Yahoo's unlawful and negligent disclosure of millions of California citizens' Yahoo account information, including their names, email addresses, telephone numbers, dates of birth, passwords and, in some cases, encrypted or unencrypted security questions and answers, in violation of California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq.* (the "CLRA"), Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, *et seq.* (the "UCL"), Customer Records Act, Cal. Civ. Code §§ 1798.80 *et. seq.* (the "CRA"), common law claims for negligence and breach of contract, and the California Constitution.

2. Yahoo is a leading Internet company that provides Internet-based services to hundreds of millions of users. According to Yahoo:

> Yahoo is a guide to digital information discovery, focused on informing, connecting, and entertaining through its search, communications, and digital content products. By creating highly personalized experiences, Yahoo helps users discover the information that matters most to them around the world – on mobile or desktop. Yahoo connects advertisers with target audiences through a streamlined advertising technology stack that combines the power of Yahoo's data, content, and technology.[1]

3. On July 25, 2016, Verizon Communications Inc. announced that it had "entered into a definitive agreement under which Verizon w[ould] acquire Yahoo's operating business for approximately $4.83 billion in cash." Verizon described Yahoo as a company that "informs, connects and entertains a global audience of more than 1 billion monthly active users** --

---

[1] *An Important Message to Yahoo Users on Security*, Yahoo (Sept. 22, 2016) <https://www.altaba.com/releasedetail.cfm?releaseid=990570> [as of June 23, 2017].

including 600 million monthly active mobile users*** through its search, communications and digital content products."[2] The acquisition officially closed on June 13, 2017, for approximately $4.5 billion—$350 million dollars less than the parties initially negotiated because of the conduct alleged herein by Plaintiffs.[3]

4. As part of its business, Yahoo collects and stores large volumes of sensitive personal information about its users, including the user's full name, gender, email addresses, cell phone numbers, birth date, passwords, and security questions linked to a user's account. Yahoo promises that it will "not rent, sell, or share personal information about [its users] with other people or non-affiliated companies except to . . . [provide] products or services, improve [Yahoo] services, contact [its users], conduct research, and provide anonymous reporting for internal and external clients."[4] Yahoo requires its users' personal information as payment in exchange for providing its services to its users, which it then uses in a manner that generates great financial profit and revenue for Yahoo.

5. Even though it requires, collects, and stores the sensitive personal information for hundreds of millions of users, Yahoo has repeatedly failed at adequately protecting its users and itself from data breaches, and continues to do so today.

6. Despite Yahoo's promises to "take[] [its users'] privacy seriously," to "limit access to personal information about [its users] to employees who [it] believe[s] reasonably need to come into contact with that information to provide products or services to [its users] or in order to do their jobs," and to "have physical, electronic, and procedural safeguards that comply with federal regulations to protect personal information about [its users]," Yahoo failed to fulfill its legal duty

---

[2] *Verizon to acquire Yahoo's operating business*, Verizon (July 25, 2016) <http://www.verizon.com/about/news/verizon-acquire-yahoos-operating-business> [as of June 23, 2017].

[3] Womack and Moritz, *Verizon Seals $4.5 Billion Yahoo Purchase as Mayer Heads Out*, Bloomberg (June 13, 2017) <https://www.bloomberg.com/news/articles/2017-06-13/verizon-seals-4-5-billion-yahoo-purchase-as-mayer-heads-out> [as of June 23, 2017].

[4] *Yahoo Privacy Center*, Yahoo (June 13, 2017) <https://policies.yahoo.com/us/en/yahoo/privacy/index.htm> [as of June 23, 2017].

to protect hundreds of millions of its users' personally identifiable information ("PII") stored in its systems.[5]

7. Specifically, on September 22, 2016, Yahoo issued a press release in which it announced that a "recent investigation" confirmed sensitive personal account information associated with at least 500 million user accounts "was stolen from the company's network in late 2014 by what it believes is a state-sponsored actor" (the "2014 Data Breach"). The information taken included "names, email addresses, telephone numbers, dates of birth, hashed passwords . . . and, in some cases, encrypted or unencrypted security questions and answers."[6]

8. On December 14, 2016, Yahoo *again* issued a press release in which it announced another separate data breach whereby "an unauthorized third party, in August 2013, stole data associated with more than one billion user accounts" (the "2013 Data Breach"). The information taken "included names, email addresses, telephone numbers, dates of birth, hashed passwords . . . and, in some cases, encrypted or unencrypted security questions and answers." Yahoo only learned of this breach in November 2016, after "law enforcement provided [it] with data files that a third party claimed was Yahoo user data," which Yahoo confirmed to be true through the use of forensic experts. As of the date of this press release, Yahoo had yet to "identify the intrusion associated" with this breach, but "believed this incident is likely distinct from the [2014 Data Breach]."[7]

9. In the same December 14, 2016 press release, Yahoo announced yet *another* data breach whereby "an unauthorized third party accessed the company's proprietary code to learn how to forge cookies[8]," allowing "an intruder to access users' accounts without a password."[9] Outside forensic experts "identified approximately 32 million user accounts for which they believe

---

[5] *Id.*

[6] *An Important Message to Yahoo Users on Security*, *supra*, fn. 1

[7] *Important Security Information for Yahoo Users*, Yahoo (Dec. 14, 2016) <https://www.altaba.com/ReleaseDetail.cfm?releaseid=1004285> [as of June 23, 2017].

[8] "A cookie is a small piece of information stored on a computer for the purpose of identifying a web browser during interaction on websites. Websites use cookies to remember and recognize details about visitors, such as website preference." (*Yahoo Security Notice December 14, 2016*, Yahoo (Dec. 14, 2016) <https://help.yahoo.com/kb/SLN27925.html> [as of June 23, 2017].)

[9] *Id.*

forged cookies were used or taken in 2015 and 2016" (the "2015-2016 Data Breach").[10] Yahoo believes it "connected some of this activity to the same state-sponsored actor believed to be responsible for the data theft the company disclosed on September 22, 2016."[11]

10. In its March 1, 2017 Form 10-K Annual Report, Yahoo admitted its "information security team had contemporaneous knowledge of the 2014 compromise of user accounts, as well as incidents by the same attacker involving cookie forging in 2015 and 2016," but, "certain senior executives did not properly comprehend or investigate, and therefore failed to act sufficiently upon, the full extent of knowledge known internally by the Company's information security team." Even though "as of December 2014, the information security team understood that the attacker had exfiltrated copies of user database backup files containing the personal data of Yahoo users . . . failures in communication, management, inquiry and internal reporting contributed to the lack of proper comprehension and handling of the 2014 Security Incident." Thus, in 2014, only "26 specifically targeted users" were notified that their information had been compromised.[12]

11. At the time of its announcement, the 2014 Data Breach was believed to be the single largest data breach in history, affecting nearly 500 million user accounts. However, Yahoo beat its own record. The 2013 Data Breach affected over **one billion** user accounts. Combined, these data breaches are the largest data breaches in history. The massive size and Yahoo's handling of the 2013 Data Breach, 2014 Data Breach, and 2015-2016 Data Breach (collectively, the "Data Breaches"), including Yahoo's failure to notify its users until years after the Data Breaches occurred and Yahoo learned about the Data Breaches, demonstrate that Yahoo recklessly and negligently disregarded its duty and obligations to safeguard and address misuse of its users' PII in violation of common law, California consumer protections statutes, and the California Constitution, and ultimately subjecting Plaintiffs and Class members to an increased, imminent risk of identity theft and fraud, and loss of value of their PII.

---

[10] *Yahoo! Inc. Form 10-K Annual Report* (Mar. 1, 2017), at p. 47, <https://www.altaba.com/secfiling.cfm?filingID=1193125-17-65791&CIK=1011006> [as of June 23, 2017].

[11] *Important Security Information for Yahoo Users*, *supra*, fn. 7.

[12] *Yahoo Security Notice December 14, 2016*, *supra*, fn. 8.

JURISDICTION AND VENUE

12. The Superior Court for the State of California, County of Orange, has jurisdiction over the entire action by virtue of the fact that this is a civil action wherein the matter in controversy, exclusive of interest and costs, exceeds the jurisdictional minimum of that Court and no Class member is a citizen of a state different from Defendant Yahoo. Yahoo has its principal place of business in California and the acts and omissions complained of in this action took place in the State of California. Venue is proper because this is a class action, the acts and/or omissions complained of took place, in whole or in part within the venue of this Court, Plaintiffs, in part, are residents of Orange County and at least part of Yahoo's obligations and liability arises in the venue of this Court. Venue is also proper pursuant to the Judicial Council of California's February 28, 2017 Order Assigning Coordination Trial Judge wherein JCCP No. 4895 was assigned to the Superior Court of California, County of Orange.

PARTIES

Plaintiff Jared Pastor

13. Plaintiff Jared Pastor is a citizen of California, and was a resident of Mission Viejo, California during the period of the Data Breaches.

14. Plaintiff Pastor has held a Yahoo user account for more than a decade which he regularly uses for personal email correspondence, including communications relating to attorney-client privilege, online purchases with credit card information, employment, and personal finances.

15. When registering for his Yahoo account, Plaintiff Pastor believed Yahoo would protect his PII, and in exchange Plaintiff Pastor provided his confidential information to Yahoo, including his name, phone number, email address, date of birth, and he created a unique password with a security question and answer to access his account.

16. As set forth above, Plaintiff Pastor uses his Yahoo user account for a variety of purposes and reasonably expected that Yahoo would protect and maintain the privacy of his confidential account information and the information contained in his email correspondence.

17. On or about September 22, 2016 and thereafter, Plaintiff Pastor learned about the Data Breaches through online news media.

18. Had Plaintiff Pastor known that Yahoo would either disclose his personal information, inadequately protect that information, or otherwise allow unauthorized persons to acquire that information without his permission, he would not have provided that information to Yahoo or signed up for Yahoo's services.

19. Given the extremely broad scope of the Data Breaches, Plaintiff Pastor's account was almost certainly amongst those included in the Data Breaches. As a result, Plaintiff Pastor purchased and continues to pay for identify theft protection and credit monitoring services from IDShield for $20.00 per month.

20. To date, Plaintiff Pastor has paid approximately $180.00 in identity theft protection and credit monitoring services or other costs related to the Data Breaches, and has spent numerous hours taking action to mitigate the impact of the Data Breaches, including researching the Data Breaches, reviewing financial and online accounts for fraud or suspicious activity, and changing his password on his Yahoo user account and other accounts linked to his Yahoo user account.

21. Plaintiff Pastor continues to monitor his accounts to prevent and/or mitigate damages resulting from the Data Breaches.

Plaintiff Brendan Quinn

22. Plaintiff Brendan Quinn is a citizen of California, and was a resident of Los Angeles, California during the period of the Data Breaches.

23. Plaintiff Quinn has held a Yahoo user account for more than a decade which he regularly uses for personal email correspondence, including communications relating to his banking, work, personal finance, income tax, and travel information.

24. When registering for his Yahoo account, Plaintiff Quinn believed Yahoo would protect his PII, and in exchange he provided confidential information to Yahoo, including his name, phone number, email address, date of birth, and he created a unique password with a security question and answer to access his account.

25. As set forth above, Plaintiff Quinn uses his Yahoo user account for a variety of purposes and reasonably expected that Yahoo would protect and maintain the privacy of his confidential account information and the information contained in his email correspondence.

26. On or about September 22, 2016 and thereafter, Plaintiff Quinn learned about the Data Breaches through news media.

27. Had Plaintiff Quinn known that Yahoo would either disclose his personal information, inadequately protect that information, or otherwise allow unauthorized persons to acquire that information without his permission, he would not have provided that information to Yahoo or signed up for Yahoo's services.

28. Given the extremely broad scope of the Data Breaches, Plaintiff Quinn's account was almost certainly amongst those included in the Data Breaches. As a result, Plaintiff Quinn purchased and continues to pay for identify theft protection and credit monitoring services from Experian for $21.95 per month.

29. To date, Plaintiff Quinn has paid approximately $197.55 in identity theft protection and credit monitoring services or other costs related to the Data Breaches, and has spent numerous hours taking action to mitigate the impact of the Data Breaches, including researching the Data Breaches, reviewing financial and online accounts for fraud or suspicious activity, researching and enrolling in identity theft protection services, and changing his password on his Yahoo user account and banking, work, and other accounts which were linked to his Yahoo user account.

30. Plaintiff Quinn continues to monitor his accounts to prevent and/or mitigate damages resulting from the Data Breaches.

Plaintiff John Bell

31. Plaintiff John Bell is a citizen of California, and was a resident of Chatsworth, California during the period of the Data Breaches.

32. Plaintiff Bell has held a Yahoo user account for more than a decade which he regularly uses for personal email correspondence, including communications relating to his personal business, employment, and online purchases, and communications with lawyers, doctors, and list serve members.

33. When registering for his Yahoo account, Plaintiff Bell believed Yahoo would protect his PII, and in exchange he provided confidential information to Yahoo, including his

name, phone number, email address, date of birth, and he created a unique password with a security question and answer to access his account.

34. As set forth above, Plaintiff Bell uses his Yahoo user account for a variety of purposes and reasonably expected that Yahoo would protect and maintain the privacy of his confidential account information and the information contained in his email correspondence.

35. On or about September 22, 2016 and thereafter, Plaintiff Bell learned about the Data Breaches, and based on information and belief, Plaintiff Bell believes he also received emails from Yahoo informing him that his personal and confidential information may have been compromised as a result of the Data Breaches.

36. Had Plaintiff Bell known that Yahoo would either disclose his personal information, inadequately protect that information, or otherwise allow unauthorized persons to acquire that information without his permission, he would not have provided that information to Yahoo or signed up for Yahoo's services.

37. Since the Data Breaches, Plaintiff Bell's Yahoo email account has been bombarded with a massive amount of unsolicited daily emails from numerous unknown sources from whom he had no prior dealings. In addition, his friends and family members have received spam emails from his account that he did not send.

38. Given the extremely broad scope of the Data Breaches, Plaintiff Bell's account was almost certainly amongst those included in the Data Breaches. As a result, Plaintiff Bell purchased and continues to pay for identify theft protection and credit monitoring services from Lifelock for $17.99 per month.

39. To date, Plaintiff Bell has not only incurred the expense of purchasing identity theft protection and credit monitoring services related to the Data Breaches, but has spent at least 30 hours mitigating the impact of the Data Breaches, including researching the Data Breaches, reviewing credit reports and financial accounts for fraud or suspicious activity, researching and enrolling in the credit monitoring services, changing his password to his Yahoo user account and other accounts linked to his Yahoo user account, and notifying and warning friends and family about spam and viral emails that may be emanating from his Yahoo email account.

40. Plaintiff Bell continues to monitor his accounts to prevent and/or mitigate damages resulting from the Data Breaches.

Plaintiff Hilary Gamache

41. Plaintiff Hilary Gamache is a citizen of California, and was a resident of Novato, California during the period of the Data Breaches.

42. Plaintiff Gamache has held a Yahoo user account for more than a decade which she regularly uses for personal email correspondence, including communications relating to her online purchases, healthcare, personal bank notifications, and other personal finance.

43. When registering for her Yahoo account, Plaintiff Gamache read Yahoo's Privacy Notice before signing up and believed Yahoo would protect her PII, and in exchange she provided confidential information to Yahoo, including her name, email address, date of birth, and she created a unique password with a security question and answer to access her account.

44. As set forth above, Plaintiff Gamache uses her Yahoo user accounts for a variety of purposes and reasonably expected that Yahoo would protect and maintain the privacy of her confidential account information and the information contained in her email correspondence.

45. On or about September 22, 2016 and thereafter, Plaintiff Gamache learned about the Data Breaches, and Plaintiff Gamache received an email from Yahoo informing her that her personal and confidential information may have been compromised as a result of the Data Breaches.

46. Had Plaintiff Gamache known that Yahoo would either disclose her personal information, inadequately protect that information, or otherwise allow unauthorized persons to acquire that information without her permission, she would not have provided that information to Yahoo or signed up for Yahoo's services.

47. Since the Data Breaches, Plaintiff Gamache has received unsolicited inquiries from numerous creditors asking to open lines of credit. This is particularly troubling because Plaintiff Gamache has had all three credit bureau agencies freeze her credit to prevent unauthorized persons from opening a line of credit without her permission. Plaintiff Gamache did not experience this issue before the Data Breaches took place.

48. Given the extremely broad scope of the Data Breaches, Plaintiff Gamache's accounts were almost certainly amongst those included in the Data Breaches.

49. To date, Plaintiff Gamache has spent numerous hours taking action to mitigate the impact of the Data Breaches, including researching the Data Breaches, reviewing credit reports and financial accounts for fraud or suspicious activity, and changing her password to her Yahoo user accounts and any other account linked to her Yahoo user accounts.

50. Plaintiff Gamache continues to monitor her accounts to prevent and/or mitigate damages resulting from the Data Breaches.

Plaintiff Jana Brabcova

51. Plaintiff Jana Brabcova is a citizen of California, and was a resident of Irvine, California during the period of the Data Breaches.

52. Plaintiff Brabcova has held a Yahoo user account for more than a decade which she regularly uses for personal email correspondence, including communications relating to her personal finances, personal income tax returns, healthcare, purchase receipts, online purchases, and other personal sensitive information.

53. When registering for her Yahoo account, Plaintiff Brabcova believed Yahoo would protect his PII, and in exchange he provided confidential information to Yahoo, including her name, phone number, email address, date of birth, and she created a unique password with a security question and answer to access her account.

54. As set forth above, Plaintiff Brabcova uses her Yahoo user account for a variety of purposes and reasonably expected that Yahoo would protect and maintain the privacy of her confidential account information and the information contained in her email correspondence.

55. On or about September 22, 2016 and thereafter, Plaintiff Brabcova learned about the Data Breaches, and Plaintiff Brabcova received an email from Yahoo informing her that her personal and confidential information may have been compromised as a result of the Data Breaches.

56. Had Plaintiff Brabcova known that Yahoo would either disclose her personal information, inadequately protect that information, or otherwise allow unauthorized persons to

acquire that information without her permission, she would not have provided that information to Yahoo or signed up for Yahoo's services.

57. Since the Data Breaches, information from Plaintiff Brabcova's Yahoo account was used to access her e-Bay account, which was then used to change her username and password, and then make an unauthorized purchase.

58. Given the extremely broad scope of the Data Breaches, Plaintiff Brabcova's account was almost certainly amongst those included in the Data Breaches.

59. To date, Plaintiff Brabcova has spent numerous hours taking action to mitigate the impact of the Data Breaches, including researching the Data Breaches, reviewing credit reports and financial accounts for fraud or suspicious activity, dealing with the unauthorized purchase, and changing her password to her Yahoo user account and any other account linked to her Yahoo user account.

60. Plaintiff Brabcova continues to monitor her accounts to prevent and/or mitigate damages resulting from the Data Breaches.

Plaintiff Michelle Bouras

61. Plaintiff Michelle Bouras is a citizen of California, and was a resident of Orange, California during the period of the Data Breaches.

62. Plaintiff Bouras has held a Yahoo user account for more than a decade which she regularly uses for personal email correspondence, including communications relating to her banking, healthcare, online shopping, purchase receipts, and personal finances.

63. When registering for her Yahoo account, Plaintiff Bouras believed Yahoo would protect her PII, and in exchange she provided confidential information to Yahoo, including her name, gender, phone number, email address, date of birth, and she created a unique password with a security question and answer to access her account.

64. As set forth above, Plaintiff Bouras uses her Yahoo user account for a variety of purposes and reasonably expected that Yahoo would protect and maintain the privacy of her confidential account information and the information contained in her email correspondence.

65. On or about September 22, 2016 and thereafter, Plaintiff Bouras learned about the Data Breaches, and Plaintiff Bouras received an email from Yahoo informing her that her personal and confidential information may have been compromised as a result of the Data Breaches.

66. Had Plaintiff Bouras known that Yahoo would either disclose her personal information, inadequately protect that information, or otherwise allow unauthorized persons to acquire that information without her permission, she would not have provided that information to Yahoo or signed up for Yahoo's services.

67. Since the Data Breaches, Plaintiff Bouras pulled a credit report to determine whether there were any fraudulent or suspicious activities, and she disassociated her Yahoo user account from all of her online accounts. In addition, subsequent to the Data Breaches, Plaintiff Bouras' friends and family members received emails from her Yahoo user account that she did not send.

68. Given the extremely broad scope of the Data Breaches, Plaintiff Bouras' account was almost certainly amongst those included in the Data Breaches.

69. To date, Plaintiff Bouras has spent approximately 25 to 30 hours taking action to mitigate the impact of the Data Breaches, reviewing credit reports and financial accounts for fraud or suspicious activity, changing her password to her Yahoo user account and other accounts linked to her Yahoo user account, and dealing with spam emails and unauthorized log-ins.

70. Plaintiff Bouras continues to monitor her accounts to prevent and/or mitigate damages resulting from the Data Breaches.

Plaintiff Reid Bracken

71. Plaintiff John Bracken is a citizen of California, and was a resident of Manhattan Beach, California during the period of the Data Breaches.

72. Plaintiff Bracken has held a Yahoo user account for more than a decade which he regularly uses for personal email correspondence, including communications relating to his online purchases with credit card information and personal finances.

73. When registering for his Yahoo account, Plaintiff Bracken believed Yahoo would protect his PII, and in exchange he provided confidential information to Yahoo, including his

name, phone number, email address, date of birth, and he created a unique password with a security question and answer to access his account.

74. As set forth above, Plaintiff Bracken uses his Yahoo user account for a variety of purposes and reasonably expected that Yahoo would protect and maintain the privacy of his confidential account information and the information contained in his email correspondence.

75. On or about September 22, 2016 and thereafter, Plaintiff Bracken learned about the Data Breaches, and Plaintiff Bracken received an email from Yahoo informing him that his personal and confidential information may have been compromised as a result of the Data Breaches.

76. Had Plaintiff Bracken known that Yahoo would either disclose his personal information, inadequately protect that information, or otherwise allow unauthorized persons to acquire that information without his permission, he would not have provided that information to Yahoo or signed up for Yahoo's services.

77. Since the Data Breaches, Plaintiff Bracken has suffered numerous instances of identity theft. For example, in 2014, Plaintiff Bracken was the victim of identity theft when one of his credit card numbers was used to make unauthorized purchases. In late 2015, Plaintiff Bracken was again a victim of identity theft when a tax return was filed with his name and personal information without his knowledge or authorization for the year of 2015. In the spring of 2017, Plaintiff Bracken was again a victim of identity theft when a second credit card in his name was used for fraudulent purchases.

78. Given the extremely broad scope of the Data Breaches, Plaintiff Bracken's account was almost certainly amongst those included in the Data Breaches.

79. To date, Plaintiff Bracken has spent numerous hours taking action to mitigate the impact of the Data Breaches, including researching the Data Breaches, reviewing credit reports and financial accounts for fraud or suspicious activity, and researching and enrolling in the credit monitoring services.

80. Plaintiff Bracken continues to monitor his accounts to prevent and/or mitigate damages resulting from the Data Breaches.

Defendant Yahoo! Inc.

81. Defendant Yahoo! Inc. is a Delaware corporation with its principal place of business in Sunnyvale, California.

82. Plaintiff is informed and believes that each Defendant named herein as a Doe is responsible in some manner for the events referred to herein which proximately caused the injuries to Plaintiffs and Class members hereinafter alleged, including but not limited to false representations and omission of material information, ignoring known data security risks, failing to provide timely notification to Plaintiffs and Class members of the Data Breaches, failing to adequately protect Plaintiff and Class members PII, and placing profits ahead of Yahoo's own legal obligations. The true names and capacities, whether individual, corporate, associate or otherwise, of Defendants Does 1-100, inclusive, are unknown to Plaintiff, who thereby sues these Defendants by such fictitious names, and will ask leave of this Court to amend this Complaint when the true names are ascertained.

FACTUAL ALLEGATIONS

A. Yahoo Requires Its Users To Provide Their PII, Which It Promises To Protect

83. Yahoo is a large technology company that provides various services to its users, including personal email accounts, fantasy sports, and news. Yahoo's services attract over one billion users per month, including 600 million monthly active mobile users.[13]

84. In order to use many of its services, Yahoo requires its users to create an account by providing Yahoo with the user's PII, including their full name, gender, email address, cell phone number, birth date, password, and various security questions linked to a user's account. For certain financial products and services offered by Yahoo, users are required to provide Yahoo with their Social Security number, asset information, and debit and credit card information. Thus, Yahoo's users purchase the right to use Yahoo's services by providing Yahoo with their PII—which has significant value for Yahoo and other businesses—in exchange for the personal use of Yahoo's services. As part of its business, Yahoo then collects and stores this PII, using it to generate

[13] *Id.*

targeted advertisements, conduct research, compile information, and provide anonymous reporting for internal and external clients. Yahoo, in part, collects this PII because it has significant value and generates substantial profits for Yahoo.[14]

85. PII is of great value and Yahoo has a duty to take every reasonable measure to protect user information and safeguard it from unlawful disclosures or theft.

86. In exchange for use of its mail service and messenger service, Yahoo also requires its users to consent to having "Yahoo's automated systems analyze all communications content (such as Mail and Messenger content including instant messages and SMS messages) to detect, among other things, certain words and phrases (Yahoo call[s] them "keywords") within these communications. Yahoo then uses this information to make "ads more relevant and useful for" its users. Yahoo admits that it "may anonymously share specific objects from a message with a 3rd party to provide a more relevant experience within your mail." In effect, as payment for the right to use its services, Yahoo requires its users to allow Yahoo to mine their personal emails and messages for use of keywords—information that is extremely valuable to any company—which it then generates an even greater profit with by targeting the user with specific advertisements that the user is more likely to select.[15] Notably, Yahoo has been sued for certain aspects of this practice. As a result of a case before the United States District Court for the Northern District of California (*In Re: Yahoo Mail Litigation*, Case No.: 13-cv-04980-LHK), Yahoo agreed to changed certain aspects of how it collects this information for a minimum of three years.[16]

87. In addition to the email scanning mentioned above, Yahoo, through its mail service, has demonstrated a lack of concern for the privacy of its users, despite its promise otherwise. For instance, reports indicate that Yahoo "secretly built a custom software program to search all of its

---

[14] *See Yahoo Privacy Center*, *supra*, fn. 4.

[15] *See Yahoo Mail FAQ*, Yahoo <https://policies.yahoo.com/us/en/yahoo/privacy/products/mail/faq/index.htm> [as of June 26, 2017].

[16] Vaas, *Yahoo email privacy lawsuit settled*, Naked Security (Sept. 1, 2016) <https://nakedsecurity.sophos.com/2016/09/01/yahoo-email-privacy-lawsuit-settled/> [as of June 26, 2017] [noting settlement resulted in zero monetary benefit to class members (other than named plaintiffs) and $4 million award in attorneys' fees for plaintiff's counsel].

customers' incoming emails for specific information provided by U.S. intelligence officials." According to security experts, "this represents the first case to surface of a U.S. Internet company agreeing to an intelligence agency's request by searching all arriving messages, as opposed to examining stored messages or scanning a small number of accounts in real time." Whereas other technology companies, such as Google, assert that they would refuse such a government request, Yahoo has demonstrated a willingness to inadequately protect, and even secretly share, the contents of its users' emails and its users' PII.[17]

88. Yahoo is and, at all relevant times, was keenly aware of the risks associated with compiling massive amounts of its users' PII and that protecting its users' PII was very important to its business. In fact, Defendant Yahoo made the following representations about its data security practices in its 2015 Annual Report:

> ***Changes in regulations or user concerns regarding privacy and protection of user data, or any failure to comply with such laws, could adversely affect our business.***
>
> Federal, state, and international laws and regulations govern the collection, use, retention, disclosure, sharing and security of data that we receive from and about our users. The use of consumer data by online service providers and advertising networks is a topic of active interest among federal, state, and international regulatory bodies, and the regulatory environment is unsettled. Many states have passed laws requiring notification to users where there is a security breach for personal data, such as California's Information Practices Act. We face similar risks in international markets where our products, services and apps are offered. **Any failure, or perceived failure, by us to comply with or make effective modifications to our policies, or to comply with any federal, state, or international privacy, data-retention or data-protection-related laws, regulations, orders or industry self-regulatory principles could result in proceedings or actions against us by governmental entities or others, a loss of user confidence, damage to the Yahoo brands, and a loss of users, advertising partners, or Affiliates, any of which could potentially have an adverse effect on our business.**
>
> In addition, various federal, state and foreign legislative or regulatory bodies may enact new or additional laws and regulations concerning privacy, data retention, data transfer and data protection issues,

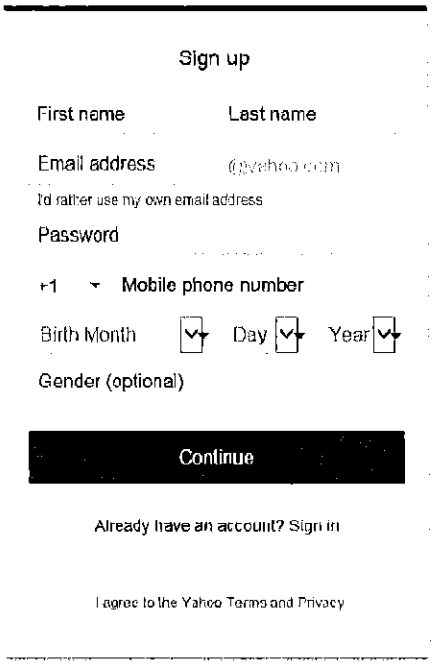
[17] *See* Menn, *Exclusive: Yahoo secretly scanned customer emails for U.S. intelligence – sources*, Reuters (Oct. 4, 2016) <http://www.reuters.com/article/us-yahoo-nsa-exclusive-idUSKCN1241YT> [as of June 26, 2017].

> including laws or regulations mandating disclosure to domestic or international law enforcement bodies, which could adversely impact our business, our brand or our reputation with users.
>
> ...
>
> ***If our security measures are breached, our products and services may be perceived as not being secure, users and customers may curtail or stop using our products and services, and we may incur significant legal and financial exposure.***
>
> Our products and services involve the storage and transmission of Yahoo's users' and customers' personal and proprietary information in our facilities and on our equipment, networks and corporate systems. Security breaches expose us to a risk of loss of this information, litigation, remediation costs, increased costs for security measures, loss of revenue, damage to our reputation, and potential liability. Outside parties may attempt to fraudulently induce employees, users, or customers to disclose sensitive information to gain access to our data or our users' or customers' data. In addition, hardware, software or applications we procure from third parties may contain defects in design or manufacture or other problems that could unexpectedly compromise network and data security. Additionally, some third parties, such as our distribution partners, service providers and vendors, and app developers, may receive or store information provided by us or by our users through applications integrated with Yahoo. If these third parties fail to adopt or adhere to adequate data security practices, or in the event of a breach of their networks, our data or our users' data may be improperly accessed, used or disclosed. Security breaches or unauthorized access have resulted in and may in the future result in a combination of significant legal and financial exposure, increased remediation and other costs, damage to our reputation and a loss of confidence in the security of our products, services and networks that could have an adverse effect on our business. We take steps to prevent unauthorized access to our corporate systems, however, because the techniques used to obtain unauthorized access, disable or degrade service, or sabotage systems change frequently or may be designed to remain dormant until a triggering event, we may be unable to anticipate these techniques or implement adequate preventative measures. If an actual or perceived breach of our security occurs, the market perception of the effectiveness of our security measures could be harmed and we could lose users and customers.[18]

89. When creating an account, Yahoo users can, but are not required to, access Yahoo's Privacy Policy by clicking a link embedded into the word "Privacy" in blue font on the bottom of the Sign-Up page:

---

[18] Yahoo! 2015 Annual Report, at p. 18 <http://files.shareholder.com/downloads/YHOO/2908978308x0x893458/96E76DB6-C10F-4514-AAB0-24BFC488B422/yahoo_ar15_annual_report.pdf> [as of Sept. 26, 2016] (emphasis added).



90. In its Privacy Policy, Yahoo represents that it will safeguard its users PII:

> **Confidentiality & Security**
>
> We limit access to personal information about you to employees 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.[19]

91. Yahoo's Privacy Policy also assures its users that it is "committed to ensuring [their] information is protected and apply safeguards in accordance with applicable law, and that "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" certain specific circumstances.[20]

92. Yahoo also promotes its promise to protect Plaintiffs and Class members' PII on its website:

---

[19] *Yahoo Privacy Center*, *supra*, fn. 4.
[20] *Id.*

> **Security at Yahoo**
>
> Protecting our systems and our users' information is paramount to ensuring Yahoo users enjoy a secure user experience and maintaining our users' trust. We have taken the following measures to protect your information:
>
> **Transport Layer Security (TLS)**
>
> We use TLS encryption when transmitting certain kinds of information, such as financial services information or payment information. An icon resembling a padlock is displayed in most browsers during TLS sessions.
>
> **Second Sign-in Verification**
>
> You may turn on a setting that requires a second piece of information such as a code sent via SMS - in addition to your password - when signing in to your account from a device or location we don't recognize. Learn more about second sign-in verification.
>
> **On-Demand Passwords**
>
> Yahoo also offers on-demand passwords. By linking your mobile device to your account, you enable Yahoo to provide you with an on-demand password sent to your mobile phone, so you don't have to remember passwords anymore. Learn more about on-demand passwords.
>
> **Secure Storage**
>
> We deploy industry standard physical, technical, and procedural safeguards that comply with relevant regulations to protect your personal information.[21]

93. When Plaintiffs and Class members signed up for Yahoo accounts, they entrusted Yahoo with their PII with the understanding that Yahoo would safeguard that information. That expectation was reinforced by Yahoo's Privacy Policy and other statements about its security, which many of its users read, were aware of, believed, and relied upon prior to signing up for their Yahoo accounts.

---

[21] *See Security at Yahoo*, Yahoo <https://policies.yahoo.com/us/en/yahoo/privacy/topics/security/index.htm> [as of June 23, 2016].

B. Yahoo Ignored Serious Risks To Its Users' PII

94. Prior to the Data Breaches, Yahoo knew that its data security was inadequate. In July 2012, unauthorized users used an SQL injection technique[22] to access the plain-text passwords of over 450,000 Yahoo! Voices (formerly known as Associated Content) users dating as far back as 2006 or earlier. The accessed information was then posted online and Yahoo encouraged Yahoo! Voice users to change their Yahoo! Voice passwords immediately. Security experts had noted that the "most worrying aspect of the attack was that the passwords for the accounts were not encrypted – meaning that any hacker could scoop up the emails and immediately start using them against other services, including Yahoo Mail."[23] Another security expert exclaimed that "Yahoo failed fatally here," and that it was "not just one specific thing that Yahoo mishandled – there [were] many different things that went wrong here. This never should have happened."[24]

95. Just a few months before the July 2012 SQL injection, Yahoo posted an article to its news website discussing numerous websites that were at risk against SQL injections and other attacks, and providing advice to websites on how to prevent such incidents.[25]

96. Still, Yahoo knowingly ignored the risks of its inadequate data security, allowing the 2012 incident and the Data Breaches to happen.

97. Under the reign of CEO Marissa Mayer (appointed in 2012), "Yahoo resisted calls for greater funding and efforts to bolster security," and "[s]ecurity was pushed to the back end . . .

---

[22] An "SQL injection is an attack technique used by hackers to insert malicious code into the database layer of a Web application. These types of attacks are typically used to plant harmful code into hacked Web sites and use that code to launch drive-by-downloads against end users." Drive-by downloading is "a catch-all name for malware that gets installed on a computer when a user simply [browses] to a (maliciously rigged) Web site." (Naraine, *Understanding Cyberspace Threats*, Bloomberg (Feb. 3, 2009) <https://www.bloomberg.com/news/articles/2009-02-03/understanding-cyberspace-threats> [as of June 23, 2017].

[23] Artur, *Yahoo Voice hack leaks 450,000 passwords*, The Guardian (July 12, 2012) <https://www.theguardian.com/technology/2012/jul/12/yahoo-voice-hack-attack-passwords-stolen> [as of June 24, 2017].

[24] Goldman, *Yahoo's password hack shows that it failed security 101*, CNN (July 12, 2012) <http://money.cnn.com/2012/07/12/technology/yahoo-hack/index.htm> [as of June 24, 2017].

[25] Shatz, *9 Things Businesses Need to Know About Web Security*, Yahoo News (Apr. 25, 2012) <https://www.yahoo.com/news/9-things-businesses-know-security-214332661.html> [as of June 24, 2017].

[for] other priorities." Instead, Yahoo was "intensely focused on trying to build 'the fastest growing startup,'" despite outwardly promising that it was "committed to keeping [its] users secure, both by continuously striving to stay ahead of ever-evolving online threats and keeping [its] users and [its] platforms safe."[26]

98. While other technology companies, such as Google, began focusing on its data security as far back as 2010 by hiring bug bounties—i.e., paying hackers that report security holes and problems in the company's data security system—and taking other measures, Yahoo waited until 2013, after the 2012 SQL incident and a series of additional spam intrusions in 2013.[27]

99. Yahoo was further warned in 2013, as a result of the disclosures of Edward J. Snowden, that it had been a "frequent target for nation-state spies." And, despite a request by Alex Stamos, Yahoo's former chief information security officer, for "Yahoo to adopt end-to-end encryption for everything," which would allow "only the parties in a conversation [to] see what was being said," Yahoo chose to ignore the request in favor of profits, allowing Yahoo to "index and search message data to provide new user services."[28]

100. And "when it came time to commit meaningful dollars to improve Yahoo's security infrastructure, Ms. Mayer repeatedly clashed with Mr. Stamos, . . . den[ying] Yahoo's security team financial resources and put off proactive security defenses, including intrusion-detection mechanisms for Yahoo's production systems." Yahoo even rejected basic security measures after a data breach, such as "an automatic reset of all user passwords, a step security experts consider standard after a breach," in order to retain its users and generate profits.[29]

---

[26] Fiegerman, *Did Yahoo do enough to prevent the massive hack?*, CNN (Sept. 23, 2016) <http://money.cnn.com/2016/09/23/technology/yahoo-hack-timeline/> [as of June 24, 2017].

[27] Perlroth & Goel, *Defending Against Hackers Took a Back Seat at Yahoo, Insiders Say*, N.Y. Times (Sept. 28, 2016) <https://www.nytimes.com/2016/09/29/technology/yahoo-data-breach-hacking.html?_r=0> [as of June 24, 2017].

[28] *Id.*

[29] *See id.*

101. Rather than focus on the data security of its users' PII during Ms. Mayer's time as CEO and during the time period of the Data Breaches, Yahoo went on an "acquisition binge, snapping up 53 companies for a total of $2.3 billion, according to a company spokesperson."[30]

102. Many companies, especially of Yahoo's size, as part of their due diligence when making an acquisition, conduct a forensic investigation of the acquired company's network and data security to address potential compatibility issues and security gaps.[31] As Yahoo had acquired approximately 53 companies during the time period of the Data Breaches, Yahoo knew or should have known what optimal data security practices consisted of and implemented such practices itself in order to protect Plaintiffs and Class members' PII. Moreover, as a result of these acquisitions and the 2012 SQL attack that resulted from an acquisition, it was foreseeable to Yahoo that a data breach would occur.

103. Eventually, Yahoo's acquisition binge resulted in Yahoo's own acquisition by Verizon, initially for $4.83 billion, but eventually finalizing the deal for $4.5 billion—$350 million dollars less than the parties initially negotiated for because of the Data Breaches.[32] And, while Ms. Mayer received a compensation package of more than $23 million when she left Yahoo as part of Verizon's acquisition,[33] Plaintiffs and Class members were left with their PII in the hands of identity thieves without any protection from Yahoo.

C. The Data Breaches

104. On September 22, 2016, Yahoo announced to the world that the sensitive personal account information of at least 500 million users was acquired in late 2014—two years before it was announced—by what Yahoo believed was a state-sponsored actor. The account information

---

[30] Kleeman, *Here's What Happened To All 53 of Marissa Mayer's Yahoo Acquisitions*, Gizmodo (June 15, 2016) <http://gizmodo.com/heres-what-happened-to-all-of-marissa-mayers-yahoo-acqu-1781980352> [as of June 24, 2017].

[31] *See Mergers & Acquisitions Risk Assessment*, FireEye <https://www.fireeye.com/services/mergers-and-acquisitions-risk-assessment.html> [as pf June 26, 2017].

[32] *Verizon Seals $4.5 Billion Yahoo Purchase as Mayer Heads Out, supra*, fn. 3.

[33] Selyukh, *Verizon Closes The Yahoo Deal; Yahoo CEO Marissa Mayer Resigns*, NPR (June 13, 2017) <http://www.npr.org/sections/thetwo-way/2017/06/13/532772877/verizon-closes-the-yahoo-deal-yahoo-ceo-marissa-mayer-resigns> [as of June 24, 2017].

included the "names, email addresses, telephone numbers, dates of birth, hashed passwords . . . and, in some cases, encrypted or unencrypted security questions and answers."[34]

105. The announcement came only after an investigation by Yahoo following reports in August 2016 that passwords, usernames, and birthdates for 200 million Yahoo accounts were found for sale on the Internet.[35] Reports at the time indicated that this may have been one of the largest data breaches in history.[36]

106. In a Securities and Exchange filing in November 2016, Yahoo admitted that it had actually known in 2014 about the state-sponsored actor that had accessed the Company's network during the Data Breach, despite failing to tell the public about this attack until nearly two years later. Hidden in this filing, Yahoo also quietly reported:

> [F]orensic experts are currently investigating certain evidence and activity that indicates an intruder, believed to be the same state-sponsored actor responsible for the [2014 Data Breach], created cookies that could have enabled such intruder to bypass the need for a password to access certain users' accounts or account information.
>
> Separately, on November 7, 2016, law enforcement authorities began sharing certain data that they indicated was provided by a hacker who claimed the information was Yahoo user account data. Yahoo will, with the assistance of its forensic experts, analyze and investigate the hacker's claim that the data is Yahoo user account data.[37]

107. Approximately one month later, on December 14, 2016, Yahoo announced an even more massive data breach whereby an unauthorized party in 2013 acquired the PII of over **one billion** user accounts. Yahoo reported that this was a separate incident from the 2014 Data Breach, and only learned about this incident after "law enforcement provided [it] with data files that a third

---

[34] *An Important Message to Yahoo Users on Security*, *supra*, fn. 1.

[35] McGoogan, *Yahoo to face 'serious questions' in UK as it's revealed hack affects eight million Britons including BT and Sky customers*, Telegraph (Sept. 23, 2016) <http://www.telegraph.co.uk/technology/2016/09/23/yahoo-to-face-serious-questions-in-uk-as-its-revealed-hack-affec/> [as of June 24, 2017].

[36] *See* Fiegerman, *Yahoo says 500 million accounts stolen*, CNN (Sept. 23, 2016) <http://money.cnn.com/2016/09/22/technology/yahoo-data-breach/index.html> [as of June 24, 2017].

[37] *Yahoo! Inc. Form 10-Q for quarterly period ended Sept. 20, 2016* (Nov. 9, 2016) at p. 40 <https://www.altaba.com/secfiling.cfm?filingID=1193125-16-764376&CIK=1011006.> [as of June 24, 2017].

party claimed was Yahoo user data." The information acquired in this breach also included the "names, email addresses, telephone numbers, dates of birth, hashed passwords . . . and, in some cases, encrypted or unencrypted security questions and answers."[38] For approximately three years this breach went undetected, leaving Plaintiffs and Class members unprotected and vulnerable to identity theft.[39]

108. Exemplifying Yahoo's reckless and completely inadequate data security is the MD5 encryption technology that Yahoo used to protect its users' passwords in 2013. As one security expert exclaimed, "[t]he MD5 hashing algorithm has been considered not just insecure, but broken, for two decades" and its use is "negligent of an organisation [sic] such as Yahoo!, which has an obligation to protect the private data of over one billion users, to be using such an outdated and ineffective control to protect the passwords of its customers." Another expert stated that "it would be pretty poor form on their part [to be] still using MD5 for hashing in 2013 and that there has "been numerous issues reported for MD5 dating back to the mid 2000s."[40]

109. In the same announcement as the 2013 Data Breach, Yahoo reported another data breach whereby "an unauthorized third party accessed the company's proprietary code to learn how to forge cookies," allowing "an intruder to access users' accounts without a password."[41] This breach affected approximately 32 million user accounts in 2015 and 2016, which Yahoo believes was connected to the same state-sponsored actor believed to be responsible for the 2014 Data Breach.[42]

110. Only until its March 1, 2017 Form 10-K Annual Report did Yahoo provide additional details of the 2014 Data Breach and the 2015-2016 Data Breach:

---

[38] *Important Security Information for Yahoo Users*, *supra*, fn. 6.

[39] Gibbs, *Security experts: 'No one should have faith in Yahoo at this point'*, Guardian (Dec. 15, 2016) <https://www.theguardian.com/technology/2016/dec/15/security-experts-yahoo-hack> [as of June 24, 2017].

[40] Pauli, *Security! experts! slam! Yahoo! management! for! using! old! crypto!*, The Register (Dec. 15, 2016) <https://www.theregister.co.uk/2016/12/15/yahoos_password_hash/> [as of June 24, 2017].

[41] *Important Security Information for Yahoo Users*, *supra*, fn. 6.

[42] *Yahoo! Inc. Form 10-K Annual Report*, *supra*, fn. 9, at p. 45.

> Based on its investigation, the Independent Committee concluded that the Company's information security team had contemporaneous knowledge of the 2014 compromise of user accounts, as well as incidents by the same attacker involving cookie forging in 2015 and 2016. In late 2014, senior executives and relevant legal staff were aware that a state-sponsored actor had accessed certain user accounts by exploiting the Company's account management tool. The Company took certain remedial actions, notifying 26 specifically targeted users and consulting with law enforcement. While significant additional security measures were implemented in response to those incidents, it appears certain senior executives did not properly comprehend or investigate, and therefore failed to act sufficiently upon, the full extent of knowledge known internally by the Company's information security team. Specifically, as of December 2014, the information security team understood that the attacker had exfiltrated copies of user database backup files containing the personal data of Yahoo users but it is unclear whether and to what extent such evidence of exfiltration was effectively communicated and understood outside the information security team. However, the Independent Committee did not conclude that there was an intentional suppression of relevant information.
>
> Nonetheless, the Committee found that the relevant legal team had sufficient information to warrant substantial further inquiry in 2014, and they did not sufficiently pursue it. As a result, the 2014 Security Incident was not properly investigated and analyzed at the time, and the Company was not adequately advised with respect to the legal and business risks associated with the 2014 Security Incident. The Independent Committee found that failures in communication, management, inquiry and internal reporting contributed to the lack of proper comprehension and handling of the 2014 Security Incident. The Independent Committee also found that the Audit and Finance Committee and the full Board were not adequately informed of the full severity, risks, and potential impacts of the 2014 Security Incident and related matters.[43]

111. Despite knowing in 2014 of the state-sponsored actor, Yahoo went two years without notifying its users that their PII had been at risk. While its users' private and personal information was potentially in the hands of identity thieves, Yahoo placed profits over notifying and protecting its users, instead spending billions on acquisitions and growth.

112. It is unclear why it took Yahoo nearly three years to discover the 2013 Data Breach, why Yahoo decided to ignore the known risks to its data security system, and why Yahoo waited approximately two years to inform Plaintiffs and Class members about the 2014 Data Breach.

---

[43] *Id. at* p. 47.

What is clear, however, is that such delay caused damage to Plaintiffs and Class members. A more timely detection and notification of the Data Breaches would have permitted Plaintiffs and Class members to act immediately in a manner to protect themselves and their PII from further harm. Instead, Yahoo's inexcusable delay increased the imminent risk of fraud and identity theft, increased the amount of money and time spent remediating the Data Breaches, and further decreased the value of Plaintiffs and Class members' PII.

113. While the Data Breaches had real effects, costing Yahoo $350 million in its acquisition by Verizon, Yahoo ultimately profited by being acquired by Verizon for nearly $4.5 billion dollars.[44] And, while the United States has "announced charges against two Russian intelligence officers and two hackers" over the 2014 and 2015-2016 Data Breaches,[45] Plaintiffs and Class members are left unprotected, having to spend time and money for the rest of their lives in order to ensure they do not become a victim to identity theft. Although Yahoo claims the acquired information did not include credit and debit card information, only discovery will be able to tell. Moreover, with the acquired information including passwords, it is reasonable to infer that unauthorized parties accessed Plaintiffs and Class members' email which likely contained banking information, credit and debit card information, medical information, health insurance information, and other types of sensitive personal information.

114. To date, Yahoo has not offered Plaintiffs and Class members any compensation from the past, present, and future harm they may experience as a result of the Data Breach. Unlike most companies victimized by data breaches, Yahoo has not even offered any form of credit monitoring services. Yahoo has utterly failed to protect Plaintiffs and Class members against fraud and identity theft which may occur as a result of the Data Breach.

---

[44] Goel, *Dissecting Marissa Mayer's $900,000-a-Week Yahoo Paycheck*, N.Y. Times (June 3, 2017) <https://www.nytimes.com/2017/06/03/technology/yahoo-marissa-mayer-compensation.html> [as of June 24, 2017].

[45] Thielman & Ackerman, *US charges two Russian spies and two hackers in Yahoo data breach*, The Guardian (March 15, 2017) <https://www.theguardian.com/technology/2017/mar/15/fbi-charges-two-russian-spies-hackers-yahoo-data-breach> [as of June 24, 2017].

115. Yahoo failed to identity, implement, maintain and/or monitor appropriate data security measures, policies, procedures, controls, protocols, and software and hardware systems to ensure the security of Plaintiffs and Class members' PII. Yahoo also failed to adequately warn and inform its users of material information regarding its data security practices and data breach incidents when they occurred. As a result, Plaintiffs and Class members were harmed by i) providing their valuable PII to Yahoo which they otherwise would not have done; ii) experiencing actual identity theft and being at a heightened risk of future identity theft and other harms; iii) spending time and money monitoring their credit history and/or paying for identity theft and credit monitoring services; iv) loss of value of their PII; and v) others harms associated with Yahoo's misrepresentations, omissions, inadequate data security, and untimely notice.

116. Additionally, Plaintiffs and Class members' PII were improperly handled and stored, and in some cases, either unencrypted or partially encrypted data was inadequately protected, readily able to be copied by data thieves, and not kept in accordance with basic security protocols.[46]

117. Had Yahoo taken appropriate security measures, the Data Breaches and the resulting injuries would not have occurred.

D. Personally Identifiable Information ("PII")

118. PII is of great value to hackers and cyber criminals and the data compromised in the Data Breaches can be used in a variety of unlawful manners.

119. PII is information that can be used to distinguish, identify, or trace an individual's identity, such as their name, Social Security number, and biometric records. This can be accomplished alone, or in combination with other personal or identifying information that is connected, or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[47]

---

[46] Bob Lord, *An Important Message About Yahoo User Security Yahoo*, YAHOO! (Sept. 22, 2016) <https://yahoo.tumblr.com/post/150781911849/an-important-message-about-yahoo-user-security> [as of June 24, 2017).

[47] Office of Mgmt. & Budget, OMB Memorandum M-07-16 (May 22, 2007) p. 1, fn. 1.

120. PII does not include only data that can be used to directly identify or contact an individual (*e.g.*, name, e-mail address), or personal data that is especially sensitive (*e.g.*, Social Security number, bank account number, payment card numbers).[48]

121. Although Yahoo has stated that the "ongoing investigation" suggests the stolen information did not include payment card data or bank account information, which will be confirmed or disproved through discovery, Yahoo nevertheless has encouraged Plaintiffs and Class members to consider placing a "security freeze" (also known as a "credit freeze") on their credit file. A security freeze is designed to prevent potential creditors from accessing an individual's credit file at the consumer reporting agencies without the individual's consent, and, according to Yahoo's notice to its users, costs roughly between $5 and $20 per freeze. Yahoo has offered no financial assistance to its users to pay for these recommended credit freezes.

122. Given the nature of the Data Breaches, it is foreseeable that the compromised PII will be used to access Plaintiffs and the Class members' user accounts, thereby providing access to additional PII or personal and sensitive information. Therefore, the compromised PII in the Data Breaches is of great value to hackers and thieves and can be used in a variety of ways. Information about, or related to, an individual for which there is a possibility of logical association with other information is of great value to hackers and thieves. Indeed, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[49] For example, different PII elements from various sources may be

---

[48] *See, e.g.*, Nat'l Inst. of Standards & Technology, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), NIST Special Publication 800-122 (April 2010) p. E.S.-1, 2-1.

[49] Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report 35-38 (Dec. 2010) <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf> [as of June 24, 2017].

able to be linked in order to identify an individual, or access additional information about or relating to the individual.[50]

123. Further, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the "mosaic effect."[51]

124. Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts particularly when they have easily-decrypted passwords and security questions. Bcrypt encryption is easily cracked by hackers and identity thieves.

125. The PII Yahoo exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breaches can be used in a variety of unlawful manners, including opening new credit and financial accounts in users' names.

126. Unfortunately for Plaintiffs and Class members, a person whose PII has been compromised may not fully experience the effects of the breach for years to come:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[52]

127. Accordingly, Plaintiffs and Class members will bear a heightened risk of injury for years to come. Identity theft is one such risk and occurs when an individuals' PII is used without his or her permission to commit fraud or other crimes.[53]

---

[50] *See id.* (evaluating privacy framework for entities collecting or using consumer data with can be "reasonably linked to a specific consumer, computer, or other device").

[51] Fed. Chief Information Officers Council, Recommendations for Standardized Implementation of Digital Privacy Controls (Dec. 2012) pp. 7-8.

[52] G.A.O., Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown (June 2007) <http://www.gao.gov/assets/270/262904.html.> [as of June 24, 2017].

[53] Fed. Trade Comm'n, Taking Charge: What To Do If Your Identity Is Stolen (April 2013) <https://www.consumer.ftc.gov/articles/pdf-0014-identity-theft.pdf> [as of June 24, 2017].

128. According to the Federal Trade Commission, "the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data."[54]

129. As a direct and proximate result of Yahoo's reckless and negligent actions, inaction, and omissions, the resulting Data Breaches, the unauthorized release and disclosure of Plaintiffs' and Class members' PII, and Yahoo's failure to properly and timely remediate the Data Breaches and give Class members proper notice of the Data Breaches, Plaintiffs and Class members are more susceptible to identity theft and have experienced, will continue to experience and will face an increased risk of experiencing the following injuries, *inter alia*:

- money and time expended to prevent, detect, contest, and repair identity theft, fraud, and/or other unauthorized uses of personal information;
- money and time lost as a result of fraudulent access to and use of their financial accounts;
- loss of use of and access to their financial accounts and/or credit;
- money and time expended to avail themselves of assets and/or credit frozen or flagged due to misuse;
- impairment of their credit scores, ability to borrow, and/or ability to obtain credit;
- lowered credit scores resulting from credit inquiries following fraudulent activities;
- money, including fees charged in some states, and time spent placing fraud alerts and security freezes on their credit records;
- costs and lost time obtaining credit reports in order to monitor their credit records;
- anticipated future costs from the purchase of credit monitoring and/or identity theft protection services;
- costs and lost time from dealing with administrative consequences of the Data Breaches, including by identifying, disputing, and seeking reimbursement for fraudulent activity, canceling compromised financial accounts and associated payment cards, and investigating options for credit monitoring and identity theft protection services;

---

[54] Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change (March 2012) <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf> [as of June 24, 2017].

- money and time expended to ameliorate the consequences of the filing of fraudulent tax returns;
- lost opportunity costs and loss of productivity from efforts to mitigate and address the adverse effects of the Data Breaches including, but not limited to, efforts to research how to prevent, detect, contest, and recover from misuse of their personal information;
- loss of the opportunity to control how their personal information is used; and
- continuing risks to their personal information, which remains subject to further harmful exposure and theft as long as Defendant Yahoo fails to undertake appropriate, legally required steps to protect the personal information in its possession.

130. The risks associated with identity theft are serious. "While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit."[55]

131. Further, criminals often trade stolen PII on the "cyber black-market" for years following a breach. Cybercriminals can post stolen PII on the internet, thereby making such information publicly available.

CLASS ACTION ALLEGATIONS

132. Plaintiffs brings this action on their own behalf, and on behalf of all persons similarly situated, pursuant to Code of Civil Procedure section 382. Plaintiffs seek to represent the following class:

> All persons who are citizens of the State of California whose personally identifiable information was accessed, compromised or acquired by unauthorized persons in the Yahoo data breaches in 2013, 2014, or 2015-2016.

133. Plaintiffs reserve the right to modify or amend the Class definition before the Court determines whether class certification is appropriate.

---

[55] True Identity Protection: Identity Theft Overview, ID Watchdog <http://www.idwatchdog.com/tikia//pdfs/Identity-Theft-Overview.pdf> [as of Sept. 23, 2016].

134. Excluded from the Class are: (i) Defendant and any entities in which Defendant has a controlling interest; (ii) any entities in which Defendant's officers, directors, or employees are employed and any of the legal representatives, heirs, successors, or assigns of Defendant; (iii) the Judge to whom this case is assigned and any member of the Judge's immediate family and any other judicial officer assigned to this case; and (iv) all governmental entities.

135. The members of the Class are so numerous, as there are nearly 40 million California residents, a large number of which were affected by the Data Breaches, that their joinder is impracticable. Their identities, and email addresses can be easily derived from Yahoo's internal records.

136. The rights of Plaintiffs, and each Class member, were violated in precisely the same manner by Yahoo's reckless and negligent actions, inaction, and omissions that caused the Data Breaches and the unauthorized release and disclosure of their PII.

137. There are questions of law and fact common to the Class as a whole. The common questions of law and fact predominate over any questions affecting only individual members of the Class, and include, without limitation:

a. Whether Yahoo had a duty to protect Plaintiffs' and the Class members' PII;

b. Whether Yahoo breached it duty to protect Plaintiffs' and the Class members' PII;

c. Whether Yahoo's breach of a legal duty caused its systems to be compromised, resulting in the loss and/or potential loss of Plaintiffs and Class members users' account data;

d. Whether Yahoo properly designed, adopted, implemented, controlled, managed and monitored data security processes, control, policies, procedures and/or protocols to protect Plaintiffs' and the Class members' PII in the Data Breach;

e. Whether Yahoo timely and adequately investigated the Data Breach and took reasonable remedial actions in response to the Data Breach';

f. Whether Yahoo failed to timely and adequately inform Plaintiffs and the Class members of the Data Breach;

g. Whether Yahoo's conduct was negligent;

h. Whether Plaintiffs and Class members are entitled to injunctive relief; and

i. Whether Plaintiffs and Class members are entitled to damages.

138. Plaintiffs' claims are typical of the claims of the Class members because Plaintiffs, like all Class members, are victims of Yahoo's wrongful actions, inaction, and omissions that caused the Data Breaches, caused the unauthorized release and disclosure of their PII. Plaintiffs and their counsel will fairly and adequately represent the interests of the Class members. Plaintiffs' counsel is highly experienced in the prosecution of complex commercial litigation, consumer class actions, and data breach cases.

139. The representative Plaintiffs will fairly and adequately represent the members of the Class and have no interests that are antagonistic to the claims of the Class. The Plaintiffs' interests in this action are antagonistic to the interests of Yahoo, and Plaintiffs will vigorously pursue the claims of the Class.

140. The representative Plaintiffs have retained counsel who are competent and experienced in consumer, data breach, and invasion of privacy class action litigation, and have successfully represented plaintiffs in complex class actions. Plaintiffs' counsel currently represents other plaintiffs in similar complex class action litigation involving wrongful disclosures and access of private information.

141. A class action provides a fair and efficient method, if not the only method, for adjudicating this controversy. The substantive claims of the representative Plaintiffs and the Class are nearly identical and will require evidentiary proof of the same kind and application of the same law. There is no plain, speedy or adequate remedy other than by maintenance of this class action.

142. A class action is superior to other available methods for the fair and efficient adjudication of this controversy because Class members number in the millions and individual joinder is impracticable. The expense and burden of individual litigation would make it impracticable or impossible for proposed Class members to prosecute their claims individually. Trial of Plaintiffs' and the Class members' claims is manageable. Unless the Class is certified, Yahoo will remain free to continue to engage in the wrongful conduct alleged herein without consequence.

143. The persons in the Class are so numerous that the joinder of all such persons individually in this case is impracticable, and the disposition of their claims in this case and as part of a single class action lawsuit, rather than hundreds or thousands of individual lawsuits, will benefit the parties and greatly reduce the aggregate judicial resources that would be spent if this matter were handled as hundreds or thousands of separate lawsuits.

144. Plaintiffs are not aware of any difficulty that will be encountered in the management of this litigation that would preclude its maintenance as a class action.

145. Absent a class action, Yahoo will retain the benefits of its wrongdoing despite its serious violations of the law and infliction of economic damages, injury, and harm on Plaintiffs and Class members.

CAUSES OF ACTION

FIRST CAUSE OF ACTION

(Violation of California Consumers Legal Remedies Act)

146. Plaintiffs re-allege and incorporate by reference all preceding factual allegations as though fully set forth herein.

147. This cause of action is brought pursuant to the California Consumers Legal Remedies Act ("CLRA"), California Civil Code § 1750, *et seq.* This cause of action does not seek monetary damages at this time and is limited solely to injunctive relief. Plaintiffs will later amend this class action Complaint to seek damages in accordance with the CLRA after providing Yahoo with notice as required by Civil Code section 1782.

148. Plaintiffs and Class members are "consumers," as the term is defined by California Civil Code section 1761, subdivision (d).

149. Plaintiffs, Class members, and Yahoo have engaged in "transactions," as that term is defined by Civil Code section 1761, subdivision (e).

150. The conduct alleged in this Complaint constitutes unfair methods of competition and unfair and deceptive acts and practices for the purpose of the CLRA, and the conduct undertaken by Yahoo was likely to deceive consumers.

151. Civil Code section 1770, subdivision (a)(5) prohibits one who is involved in a transaction from "[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have."

152. Yahoo violated this provision by representing that Yahoo would take appropriate measures to protect Plaintiffs' and the Class members' PII, take its user's privacy seriously, limit access its users' PII, and comply with the law. Yahoo however improperly handled, stored, or protected either unencrypted or partially encrypted data consisting of its users' PII. Yahoo also failed to adequately notify its users of the Data Breaches, instead choosing to hide such information in favor of its acquisition and profits, causing Plaintiffs additional harm.

153. Civil Code section 1770, subdivision (a)(7) prohibits one who is involved in a transaction from "[r]epresenting that goods or services are of a particular standard, quality, or grade . . . if they are of another."

154. Yahoo violated this provision by representing that it its data security would adequately protect its users' personal information, and would not allow that information to be provided to any unauthorized parties. Moreover, as a result of the 2012 SQL incident, its numerous acquisitions, and its 2014 knowledge of the state-sponsored actors, Yahoo knew and should have known that its data security was inadequate when it made such representations and material omissions to Plaintiffs and Class members. And, Yahoo made such representations and omission in order to retain its users and profits, and secure its own acquisition.

155. Plaintiffs and the Class members relied upon Yahoo's representations and were induced to sign up for a Yahoo user account, and provide their PII which contains value in order to obtain services from Yahoo.

156. As a result of engaging in such conduct, Yahoo has violated Civil Code section 1770.

157. Pursuant to Civil Code section 1780, subdivisions (a)(2) and (a)(5), Plaintiffs seek an order of this Court that includes, but is not limited to, an order enjoining Yahoo from continuing to engage in unlawful, unfair, or fraudulent business practices or any other act prohibited by law, and requiring Yahoo to take remedial measures to ensure the Data Breaches and its improper

business practices in monitoring, remediating and responding to the Data Breaches will not happen again.

158. Plaintiffs and the Class members suffered injuries caused by Yahoo's misrepresentations and omissions, because they provided their PII believing that Yahoo would adequately protect this information.

159. Plaintiffs and Class members may be irreparably harmed and/or denied an effective and complete remedy if such an order is not granted.

160. The unfair and deceptive acts and practices of Yahoo, as described above, present a serious threat to Plaintiffs and members of the Class.

SECOND CAUSE OF ACTION

(Violation of Unfair Competition Law California Business and Professional Code Sections 17200 *et seq.*)

161. Plaintiffs re-allege and incorporate by reference all preceding factual allegations as though fully set forth herein.

162. Plaintiffs brings this claim on behalf of themselves and the Class.

163. The California Unfair Competition Law, Cal. Bus. & Prof. Code sections 17200 *et seq*. ("UCL"), prohibits any "unlawful," "fraudulent" or "unfair" business act or practice and any false or misleading advertising, as defined by the UCL and relevant case law.

164. By reason of Yahoo's above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized disclosure of Plaintiffs and Class members' PII, Yahoo engaged in unlawful, unfair and fraudulent practices within the meaning of the UCL.

165. Yahoo's business practices as alleged herein are unfair because they offend established public policy and are immoral, unethical, oppressive, unscrupulous and substantially injurious to consumers, in that the private and confidential PII of Plaintiffs and Class members has been compromised for all to see, use, or otherwise exploit.

166. Yahoo's practices were unlawful and in violation of Civil Code sections 1798 *et seq.* and Defendant Yahoo's own privacy policy because Yahoo failed to take reasonable measures

to protect Plaintiffs' and Class members' PII and failed to take remedial measures such as notifying its users when it first discovered that their PII may have been compromised.

167. Yahoo's business practices as alleged herein are fraudulent because they are likely to deceive consumers into believing that the PII they provide to Defendant Yahoo will remain private and secure, when in fact it was not private and secure, and that Yahoo would take proper measures to investigate and remediate the Data Breaches, when Yahoo did not.

168. Plaintiffs and Class members suffered (and continue to suffer) injury in fact and lost money or property as a direct and proximate result of Yahoo's above-described wrongful actions, inaction, and omissions including, *inter alia*, the unauthorized release and disclosure of their PII and lack of notice.

169. Yahoo's above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs' and Class members' PII also constitute "unfair" business acts and practices within the meaning of Business & Professions Code sections 17200 *et seq.*, in that Yahoo's conduct was substantially injurious to Plaintiffs and Class members, offensive to public policy, immoral, unethical, oppressive and unscrupulous, and the gravity of Yahoo's conduct outweighs any alleged benefits attributable to such conduct.

170. But for Yahoo's misrepresentations and omissions, Plaintiffs and Class members would not have provided their PII to Yahoo, or would have insisted that their PII be more securely protected.

171. As a direct and proximate result of Yahoo's above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs and Class members' PII, they have been injured as follows: (1) the loss of the opportunity to control how their PII is used; (2) the diminution in the value and/or use of their PII entrusted to Yahoo; (3) the increased, imminent risk of fraud and identity theft; (4) the compromise, publication, and/or theft of their PII; and (5) costs associated with monitoring their PII, amongst other things.

172. Plaintiffs takes upon themselves enforcement of the laws violated by Yahoo in connection with the reckless and negligent disclosure of PII. There is a financial burden incurred

in pursuing this action and it would be against the interests of justice to penalize Plaintiffs by forcing them to pay attorneys' fees and costs from the recovery in this action. Therefore, an award of attorneys' fees and costs is appropriate under Code of Civil Procedure section 1021.5.

THIRD CAUSE OF ACTION

(Violation of California Customer Records Act, Cal. Civ. Code §§ 1798.80 *et seq.*)

173. Plaintiffs re-allege and incorporate by reference all preceding factual allegations as though fully set forth herein.

174. "[T]o ensure that personal information about California residents is protected," Civil Code section 1798.81.5 requires that any business that "owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

175. Yahoo owns, maintains, and licenses personal information, within the meaning of section 1798.81.5, about Plaintiffs and the Class.

176. Yahoo violated Civil Code section 1798.81.5 by failing to implement reasonable measures to protect Plaintiffs' and Class members' personal information, to remediate the Data Breaches, and to timely and adequately notify Class members.

177. As a direct and proximate result of Yahoo's violations of section 1798.81.5 of the California Civil Code, the Data Breaches described above occurred and harms stemming from the Data Breaches were not timely cured.

178. In addition, California Civil Code section 1798.82(a) provides that "[a] person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of 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 unreasonable delay . . ."

179. Section 1798.2(b) provides that "[a] person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

180. Defendant Yahoo is a business that owns or licenses computerized data that includes personal information as defined by Civil Code sections 1798.80 *et seq*.

181. In the alternative, Defendant Yahoo maintains computerized data that includes personal information that Defendant Yahoo does not own as defined by Civil Code sections 1798.80 *et seq*.

182. Plaintiffs' and Class members' personally identifiable information (including but not limited to names, addresses, and Social Security numbers) includes personal information covered by Civil Code § 1798.81.5(d)(1).

183. Because Yahoo reasonably believed that Plaintiffs' and the Class members' personal information was acquired by unauthorized persons during the Data Breaches, it had an obligation to disclose the Data Breaches in a timely and accurate fashion under Civil Code section 1798.82, subdivision (a), or in the alternative, under Civil Code section 1798.82, subdivision (b).

184. By failing to disclose the Data Breaches in a timely and accurate manner, Yahoo violated Civil Code section 1798.82.

185. As a direct and proximate result of Defendant's violations of Civil Code sections 1798.81.5 and 1798.82, Plaintiffs and Class members suffered the damages described above including, but not limited to, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased imminent risk of fraud and identity theft, and loss of value of their personally identifying information.

186. Plaintiffs and Class members seek relief under Civil Code section 1798.84 including, but not limited to, actual damages, to be proven at trial, and injunctive relief.

FOURTH CAUSE OF ACTION

(Negligence)

187. Plaintiffs re-allege and incorporate by reference all preceding factual allegations as though fully set forth herein.

188. Plaintiffs bring this claim on behalf of themselves and the Class.

189. Plaintiffs and Class members were required to provide Yahoo with certain PII in connection with their Yahoo user accounts. Yahoo collected and stored this information including their names, birthdays and passwords.

190. Yahoo had a duty to Plaintiffs and Class members to safeguard and protect their PII, including the duty to timely and reasonably investigate and remediate Data Breaches and notify Class members timely and adequately concerning the Data Breaches.

191. Yahoo assumed a duty of care to use reasonable means to secure and safeguard this PII, to prevent its disclosure, to guard it from theft, to detect any attempted or actual breach of its systems, to timely and reasonably investigate and remediate Data Breaches and to notify Class members timely and adequately concerning the Data Breaches.

192. Yahoo had full knowledge about the sensitivity of Plaintiffs' and Class members' PII, as well as the type of harm to could occur if such PII was wrongfully disclosed, if disclosure was not timely or adequately remediated, or if Class members were not timely and adequately alerted of the Data Breaches.

193. Yahoo had a special relationship with Plaintiffs and Class members as a result of being entrusted with their PII, which provided an independent duty of care. Plaintiffs' and Class members' willingness to entrust Yahoo with their PII was predicated on the understanding that Yahoo would take adequate security precautions. Moreover, Yahoo was capable of protecting its networks and systems, and the PII it stored on them, from unauthorized access, but failed to do so time and time again. Yahoo's repeated security incidents and its numerous acquisitions demonstrate that the harm to Plaintiffs and Class members was foreseeable. The massive size of the Data Breaches, Yahoo's failure to disclose the Data Breaches to the public when it first discovered the intrusions, and its lack of remediation following the Data Breaches demonstrate

that Yahoo is morally to blame for the Data Breaches, and it cannot be trusted to prevent future data breaches.

194. Yahoo had a duty to use ordinary care in activities from which harm might be reasonably anticipated in connection with user PII data and Data Breaches.

195. Yahoo breached its duty of care by failing to secure and safeguard the PII of Plaintiffs and Class members, failing to timely and reasonably investigate and remediate Data Breaches and failing to timely and adequately inform Class members concerning the Data Breaches. Yahoo negligently stored and/or maintained its systems.

196. Further, Yahoo, by and through its above negligent actions and/or inaction, further breached its duties to Plaintiffs and Class members by failing to design, adopt, implement, control, manage, monitor, remediate, investigate and audit its processes, controls, policies, procedures, vulnerabilities and protocols for complying with the applicable laws and safeguarding and protecting Plaintiffs' and Class members' PII within its possession, custody and control.

197. Plaintiffs and the other Class members have suffered harm as a result of Yahoo's negligence. Plaintiffs and Class members' loss of control over their compromised PII has subjected and continues to subject each of them to harms stated herein, including but not limited to a greatly enhanced risk of identity theft, fraud, and myriad other types of fraud and theft stemming from either use of the compromised information, and access to their user accounts.

198. It was reasonably foreseeable—in that Yahoo knew or should have known—that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII would result in its release and disclosure to unauthorized third parties who, in turn wrongfully used such PII, or disseminated it to other fraudsters for their wrongful use and for no lawful purpose. It was reasonably foreseeable—in that Yahoo knew or should have known—that its failure to timely and reasonably investigate and remediate the Data Breaches and to notify Class members in a timely and adequate manner concerning the Data Breaches, would result in further release and disclosure of the information to unauthorized third parties, as well as further exposure to harms due to Class members' delay in addressing and attempting to cure risks associated with identity theft and misuse of their information by third parties.

199. But for Yahoo's negligent and wrongful breach of its responsibilities and duties owed to Plaintiffs and Class members, their PII would not have been compromised and the harms alleged herein would not have been incurred.

200. As a direct and proximate result of Yahoo's above-described wrongful actions, inaction, and omissions, the resulting Data Breaches, and the unauthorized release and disclosure of Plaintiffs' and Class members' PII, they have incurred (and will continue to incur) the above-referenced economic damages, and other actual injury and harm—for which they are entitled to compensation. Yahoo's wrongful actions, inaction, and omissions constituted (and continue to constitute) common law negligence/negligent misrepresentation.

201. Plaintiffs and Class members are entitled to injunctive relief as well as actual and punitive damages.

FIFTH CAUSE OF ACTION

(Breach of Contract)

202. Plaintiffs re-allege and incorporate by reference all preceding factual allegations as though fully set forth herein.

203. Plaintiffs bring this claim on behalf of themselves and the Class.

204. Yahoo's Privacy Policy, which is incorporated in Yahoo's Terms of Service, forms a contract between Yahoo and Yahoo account holders.

205. Yahoo requires account holders to provide various types of personal information in connection with Yahoo user accounts.

206. Yahoo's Privacy Policy explicitly states that Yahoo "has physical, electronic, and procedural safeguards that comply with federal regulations to protect personal information about you."[56] Yahoo also states that it will "not rent, sell or share personal information about you with other people or non-affiliated companies except to . . . [provide] products or services, improve our

[56] *Supra*, fn. 4.

services, contact you, conduct research, and provide anonymous reporting for internal and external clients."[57]

207. Under the terms of the agreement, Yahoo was obligated to maintain the security of Plaintiffs and the Class members.

208. Plaintiffs and Class members provided their PII in connection with their Yahoo user accounts, and allowed Yahoo to scan their emails for keywords.

209. Plaintiffs and Class members relied upon these terms and would not have disclosed their PII without assurances that it would be properly safeguarded.

210. Plaintiffs and Class members fulfilled their obligations under the contract by providing their PII to Yahoo.

211. However, Yahoo failed to safeguard and protect Plaintiffs' and Class members' PII. In permitting the Data Breaches, Yahoo breached the terms of its Privacy Policy and other statements it made regarding its users' privacy. For instance, in its Privacy Policy, Yahoo asserted that it "believe[s] 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." Although Yahoo shared its users' PII with identity thieves, it did not do so in order to investigate, prevent, or take action regarding illegal activities or suspected frauds. Yahoo also failed to adequately remediate the Data Breaches and notify its users that their PII may have been compromised, despite its obligation to do so as required by law.

212. As the direct and proximate result of Yahoo's breaches of the contracts between Yahoo and Plaintiffs and Class members, Plaintiffs and Class members sustained actual losses and damages as described above.

213. Accordingly, Plaintiffs, on behalf of themselves and the Class members, respectfully request this Court to award all relevant damages for Yahoo's breach of contract.

---

[57] *Id.*

SIXTH CAUSE OF ACTION

(Invasion of Privacy)

214. Plaintiffs re-allege and incorporate by reference all preceding factual allegations as though fully set forth herein.

215. Plaintiffs bring this claim on behalf of themselves and the Class.

216. Plaintiffs and Class members have a legally protected privacy interest in their PII that Defendant Yahoo required them to provide and stored.

217. Plaintiffs and Class members reasonably expected that their PII would be protected and secured from unauthorized parties, would not be disclosed to any unauthorized parties or disclosed for any improper purpose.

218. Defendant Yahoo unlawfully invaded the privacy rights of Plaintiffs and Class members by (a) failing to adequately secure their PII from disclosure to unauthorized parties for improper purposes; (b) disclosing their PII to unauthorized parties in a manner that is highly offensive to a reasonable person; and (c) disclosing their PII to unauthorized parties without the informed and clear consent of Plaintiffs and Class members. Further, Yahoo invaded the privacy rights of Plaintiffs and Class members by failing to adequately or timely take steps to remediate the Data Breaches, or provide Class members notice of the Data Breaches, once Yahoo possessed knowledge to a substantial certainty that the Data Breaches were occurring and that Class members were being harmed. This invasion into the privacy interest of Plaintiffs and Class members is serious and substantial.

219. In failing to adequately secure Plaintiffs' and Class members' PII, Defendant Yahoo acted in reckless disregard of their privacy rights. Yahoo knew or should have known that their substandard data security measures are highly offensive to a reasonable person in the same position as Plaintiffs and Class members.

220. Yahoo violated Plaintiffs' and Class members' right to privacy under the common law as well as under state law, including but not limited to the California Constitution, Article I, Section I.

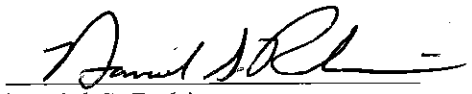
221. As a direct and proximate result of Yahoo's unlawful invasions of privacy, Plaintiffs' and Class members' PII has been viewed or is at imminent risk of being viewed, and their reasonable expectations of privacy have been intruded upon and frustrated. Plaintiffs and the Class have suffered injury as a result of Defendant's unlawful invasions of privacy and are entitled to appropriate relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Class pray for judgment as follows:

1. For an Order certifying the proposed Class pursuant to California Civil Code Section 382, requiring notice thereto to be paid by Defendant and appointing Plaintiffs and their counsel to represent the Class;
2. For appropriate injunctive relief and/or declaratory relief, including, but not limited to, an order requiring Defendant to immediately secure and fully encrypt all confidential information, to cease negligently storing, handling, and securing its users confidential information, to notify users whose PII is wrongly disclosed in an expedient and timely manner and to provide identity theft monitoring;
3. Adjudging and decreeing that Defendant Yahoo has engaged in the conduct alleged herein;
4. For compensatory and general damages according to proof on certain causes of action;
5. For reimbursement, restitution and disgorgement on certain causes of action;
6. For both pre- and post-judgment interest at the maximum allowable rate on any amounts awarded;
7. For costs of the proceedings herein;
8. For reasonable attorneys' fees as allowed by California Code of Civil Procedure Section 1021.5, and any other applicable statutes; and
9. For any and all such other and further relief that this Court may deem just and proper, including, but not limited to, punitive or exemplary damages.

Dated: June 27, 2017

By: 

Daniel S. Robinson
Wesley K. Polischuk
ROBINSON CALCAGNIE, INC.
19 Corporate Plaza Drive
Newport Beach, CA 92660
Telephone: (949) 720-1288
Facsimile: (949) 720-1292
drobinson@robinsonfirm.com
wpolischuk@robinsonfirm.com

Brian D. Chase
Jerusalem F. Beligan
BISNAR CHASE LLP
1301 Dove Street, Suite 120
Newport Beach, CA 92626
Telephone: (949) 752-2999
Facsimile: (949) 752-2777
bchase@bisnarchase.com
jbeligan@bisnarchase.com

Plaintiffs' Co-Lead Counsel

Jeremiah Frei-Pearson (*Pro Hac Vice*)
D. Greg Blankinship (*Pro Hac Vice*)
FINKELSTEIN, BLANKINSHIP FREI-PEARSON & GARBER, LLP
445 Hamilton Avenue, Suite 605
White Plains, NY 10601
Telephone: (914) 298-3281
Facsimile: (914) 908-6709
jfrei-pearson@fbfglaw.com
gblankinship@fbfglaw.com

Eric A. Grover
Robert W. Spencer
KELLER GROVER LLP
1965 Market Street
San Francisco, CA 94103
Telephone: (415) 543-1305
Facsimile: (415) 543-7861
eagrover@kellergrover.com
rspencer@kellergrover.com

Plaintiffs' Co-Liaison Counsel

Neil B. Fineman
Phillip R. Poliner
FINEMAN POLINER LLP
155 North Riverview Drive
Anaheim Hills, CA 92808
Telephone: (714) 620-1125
Facsimile: (714) 701-0155
Neil@FinemanPoliner.com
Phillip@FinemanPoliner.com

Robert Samini
SAMINI SCHEINBERG PC
840 Newport Center Dr., Suite 700
Newport Beach, CA 92660
Telephone: (949) 724-0900
Facsimile: (949) 724-0901

Nathan M. Smith
BROWN NERI, SMITH & KHAN LLP
11766 Wilshire Blvd, Suite 1670
Los Angeles, CA 90025
Telephone: (310) 593-9890
Facsimile: (310) 593-9980
nate@bnsklaw.com

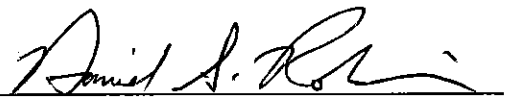
Brian S. Kabateck
Natalie Pang
KABATECK BROWN KELLNER LLP
Engine Company No. 28 Building
644 South Figueroa Street
Los Angeles, CA 90017
Telephone: (213) 217-5000
Facsimile: (213) 217-5010
bsk@kbklawyers.com
lm@kbklawyers.com

Plaintiffs' Steering Committee

DEMAND FOR JURY TRIAL

Plaintiffs hereby demands trial by jury of all claims and causes of action in this lawsuit to which they are so entitled.

Dated: June 27, 2017

By: 

Daniel S. Robinson
Wesley K. Polischuk
ROBINSON CALCAGNIE, INC.
19 Corporate Plaza Drive
Newport Beach, CA 92660
Telephone: (949) 720-1288
Facsimile: (949) 720-1292
drobinson@robinsonfirm.com
wpolischuk@robinsonfirm.com

BISNAR | CHASE LLP
BRIAN D. CHASE
bchase@bisnarchase.com
JERUSALEM F. BELIGAN
jbeligan@bisnarchase.com
1301 Dove Street, Suite 120
Newport Beach, CA 92660
Telephone: (949) 752-2999
Facsimile: (949) 752-2777

Plaintiffs' Co-Lead Counsel

Jeremiah Frei-Pearson
D. Greg Blankinship
FINKELSTEIN, BLANKINSHIP FREI-PEARSON & GARBER, LLP
445 Hamilton Avenue, Suite *605*
White Plains, NY 10601
Telephone: (914) 298-3281
Facsimile: (914) 908-6709
jfrei-pearson@fbfglaw.com
gblankinship@thfglaw.com

Eric A. Grover
Robert W. Spencer
KELLER GROVER LLP
1965 Market Street
San Francisco, CA 94103
Telephone: (415) 543-1305
Facsimile: *(415)* 543-7861
eagroverkellergrover.com

rspencer@kellergrover.com

Plaintiffs' Co-Liaison Counsel

Neil B. Fineman
Phillip R. Poliner
FINEMAN POLIINER LLP
155 North Riverview Drive
Anaheim Hills, CA 92808
Telephone: (714) 620-1125
Facsimile: (714) 701-0155
Neil@FinemanPoliner.com
Phillip@FinemanPoliner.com

Robert Samini
SAMINI SCHEINBERG PC
840 Newport Center Dr., Suite 700
Newport Beach, CA 92660
Telephone: (949) 724-0900
Facsimile: (949) 724-0901

Nathan M. Smith
BROWN NERI, SMITH & KHAN LLP
11766 Wilshire Blvd, Suite 1670
Los Angeles, CA 90025
Telephone: (310) 593-9890
Facsimile: (310) 593-9980
nate@bnsklaw.com

BRIAN S. KABATECK
NATALIE S. PANG
KABATECK BROWN KELLNER LLP
Engine Company No. 28 Building
644 South Figueroa Street
Los Angeles, CA 90017
Telephone: (213) 217-5000
Facsimile: (213) 217-5010
bsk@kbklawyers.com
np@kbklawyers.com

Plaintiffs' Steering Committee

PROOF OF SERVICE

STATE OF CALIFORNIA, COUNTY OF ORANGE

I certify that I am over the age of 18 years and not a party to the within action; that my business address is:

ROBINSON CALCAGNIE, INC.
19 Corporate Plaza Drive
Newport Beach, CA 92660

On June 27, 2017, I served the foregoing document described as:

CONSOLIDATED CLASS ACTION COMPLAINT; JURY TRIAL DEMAND

on the parties in this action as stated on the attached service list as follows:

___ (By Federal Express) Said documents were delivered to an authorized courier or driver authorized by the express service carrier to receive documents with delivery fees paid or provided for.

_X_ (By Mail) I am "readily familiar" with the firm's practice of collection and processing correspondence for mailing. Under practice, it would be deposited with the U.S. Postal Service on that same day with postage thereon fully prepaid at Newport Beach, California in the ordinary course of business. I am aware that on motion of the party served, service is presumed invalid if postal cancellation date or postage meter date is more than one day after date of deposit for mailing in affidavit.

___ (By Personal Service) I caused each document to be delivered by hand to the home of the addressee.

___ (By FAX) I caused each document to be sent by FAX to the parties listed on the attached mail list.

___ (By Electronic Service) I caused each document to be sent by electronic service by transmitting a true and correct PDF version as indicated above of the foregoing document(s) via each individual's email.

_X_ STATE: I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

___ FEDERAL: I declare that I am employed in the office of a member of a Bar of this Court at whose direction the service was made.

Executed on this 27th day of June, 2017 at Newport Beach, California.

Jennifer D. Rogers

SERVICE LIST

Ann Marie Mortimer, Esq. Jason J. Kim, Esq. Kirk A. Hornbeck, Esq. HUNTON & WILLIAMS, LLP 550 S. Hope Street, Suite 2000 Los Angeles, CA 90071-2627 (213) 532-2000; Fax: (213) 532-2020 amortimer@hunton.com kimj@hunton.com khornbeck@hunton.com	*Attorneys for Defendant Yahoo! Inc.* *(All Cases)*
Brian D. Chase Jerusalem F. Beligan BISNAR | CHASE LLP 1301 Dove Street, Suite 120 Newport Beach, CA 92626 Telephone: (949) 752-2999 Facsimile: (949) 752-2777 bchase@bisnarchase.com jbeligan@bisnarchase.com	*Plaintiffs' Co-Lead Counsel*
Jeremiah Frei-Pearson FINKELSTEIN, BLANKINSHIP FREI-PEARSON & GARBER, LLP 445 Hamilton Avenue, Suite 605 White Plains, NY 10601 Telephone: (914) 298-3281 Facsimile: (914) 908-6709 jfrei-pearson@fbfglaw.com gblankinship@fbfglaw.com	*Plaintiffs' Co-Liaison Counsel*
Eric A. Grover KELLER GROVER LLP 1965 Market Street San Francisco, CA 94103 Telephone: (415) 543-1305 Facsimile: (415) 543-7861 eagrover@kellergrover.com cer@kellergrover.com	*Plaintiffs' Co-Liaison Counsel*

Neil B. Fineman Phillip R. Poliner FINEMAN POLINER LLP 155 North Riverview Drive Anaheim Hills, CA 92808 Telephone: (714) 620-1125 Facsimile: (714) 701-0155 Neil@FinemanPoliner.com Phillip@FinemanPoliner.com	*Plaintiffs' Steering Committee*
Nathan M. Smith BROWN NERI, SMITH & KHAN LLP 11766 Wilshire Blvd, Suite 1670 Los Angeles, CA 90025 Telephone: (310) 593-9890 Facsimile: (310) 593-9980 nate@bnsklaw.com	*Plaintiffs' Steering Committee*
Robert Samini SAMINI SCHEINBERG PC 840 Newport Center Dr., Suite 700 Newport Beach, CA 92660 Telephone: (949) 724-0900 Facsimile: (949) 724-0901 bsamini@saminilaw.com	*Plaintiffs' Steering Committee*
Brian S. Kabateck Natalie Pang KABATECK BROWN KELLNER LLP Engine Company No. 28 Building 644 South Figueroa Street Los Angeles, CA 90017 Telephone: (213) 217-5000 Facsimile: (213) 217-5010 bsk@kbklawyers.com np@kbklawyers.com	*Plaintiffs' Steering Committee*

PROOF OF SERVICE