

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

**POMERANTZ LLP**

Jeremy A. Lieberman (pro hac vice)  
Emma Gilmore (pro hac vice)  
600 Third Avenue  
New York, NY 10016  
Telephone: (212) 661-1100  
E-mail: jalieberman@pomlaw.com  
egilmore@pomlaw.com

**GLANCY PRONGAY & MURRAY LLP**

Joshua L. Crowell (295411)  
Jennifer Leinbach (#281404)  
1925 Century Park East, Suite 2100  
Los Angeles, CA 90067  
Telephone: (310) 201-9150  
E-mail: jcrowell@glancylaw.com

- additional counsel on signature page -

**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA**

IN RE YAHOO! INC. SECURITIES  
LITIGATION

Case No. 17-CV-00373 (LHK)

**FIRST AMENDED CLASS ACTION  
COMPLAINT FOR VIOLATIONS OF  
THE FEDERAL SECURITIES LAWS**

THIS DOCUMENT RELATES TO:  
ALL ACTIONS

JURY TRIAL DEMANDED

TABLE OF CONTENTS

1 NATURE OF THE ACTION ..... 1  
 2  
 3 JURISDICTION AND VENUE ..... 4  
 4  
 5 PARTIES ..... 5  
 6  
 7 SUBSTANTIVE ALLEGATIONS ..... 5  
 8     Background ..... 5  
 9     Private Information Is Valuable to Criminals ..... 6  
 10     Yahoo Was Required to Timely and Accurately Disclose All of Its Security Vulnerabilities... 10  
 11     During the Class Period, Yahoo Struggled to Stay Afloat..... 16  
 12     Despite Being Repeatedly Hacked During the Class Period, Yahoo Refused to Invest  
 13         in Needed Security Upgrades..... 21  
 14     The 2013 Data Breach ..... 28  
 15     The 2014 Data Breach ..... 32  
 16     The Forged Cookie Data Breach..... 37  
 17     Defendants Had Contemporaneous Knowledge of the Breaches ..... 38  
 18     Yahoo Is Assailed for Failure to Fulfill Its Disclosure Obligations ..... 44  
 19     The Breaches Jeopardized Yahoo’s Transaction with Verizon ..... 48  
 20     Yahoo Faces Significant Financial Exposure and Reputational Harm ..... 50  
 21     Materially False and Misleading Statements Issued During the Class Period..... 51  
 22         A. False and Misleading Statements Made in 2013..... 52  
 23         B. False and Misleading Statements Made in 2014..... 57  
 24         C. False and Misleading Statements Made in 2015..... 68  
 25         D. False and Misleading Statements Made in 2016..... 77  
 26     The Truth Begins to Emerge..... 84  
 27 ADDITIONAL SCIENTER ALLEGATIONS..... 95  
 28 PLAINTIFFS’ CLASS ACTION ALLEGATIONS..... 98  
 COUNT I ..... 101  
     Violation of Section 10(b) of the Exchange Act and Rule 10b-5 Against All Defendants ..... 101  
 COUNT II..... 103  
     Violation of Section 20(a) of the Exchange Act Against The Individual Defendants..... 103  
 PRAYER FOR RELIEF ..... 104



1 3. Yahoo's products and services involve the storage and transmission of Yahoo's users'  
2 and customers' personal and proprietary information, including the users' names, email addresses,  
3 telephone numbers, birth dates, passwords, social security numbers, security questions linked to a user's  
4 account, and credit and/or debit card information. Yahoo trumpets its access to users' private  
5 information in an effort to appeal to advertisers through its ability to conduct targeted advertisements.  
6 While a user's private information is indispensable and the most valuable asset to Yahoo's business, it  
7 is also "as good as gold" to identity thieves, who exploit it for a variety of nefarious reasons, including  
8 draining the bank accounts of the victims whose information they misappropriated, claiming their  
9 disability benefits, obtaining a driver license in their name, and committing tax fraud.  
10

11 4. During the Class Period, Yahoo repeatedly warned in its public filings that cybersecurity  
12 attacks represented a material operating risk, warning that "[i]f our security measures are breached, our  
13 products and services may be perceived as not being secure, users and customers may curtail or stop  
14 using our products and services, and we may incur significant legal and financial exposure."  
15 Understanding the gravity of identity theft, Defendants publicly acknowledged that "there is nothing  
16 more important to [Yahoo] than protecting our users' privacy." To that end, Yahoo proclaimed on its  
17 official website that "[t]ime is of the essence when we discover" security vulnerabilities and  
18 "commit[ed] to publicly disclos[e] . . . [on its website] the vulnerabilities we discover within 90 days."  
19 Indeed, almost every state in the country makes it illegal for any company to improperly delay notifying  
20 customers of data breaches because companies have little to no incentive to disclose hacks voluntarily,  
21 given the financial and reputational harm a security breach can cause. Similarly, the Securities and  
22 Exchange Commission requires "timely, comprehensive, and accurate information" about cybersecurity  
23 incidents, particularly where a registrant experienced a cyber attack compromising customer data.  
24  
25

26 5. Defendants recently admitted they had contemporaneous knowledge of the breaches:  
27 "the Company's information security team had contemporaneous knowledge of the 2014 compromise  
28

1 of user accounts, as well as incidents by the same attacker involving cookie forging in 2015 and 2016.  
2 In late 2014, senior executives and relevant legal staff were aware that a state-sponsored actor had  
3 accessed certain user accounts by exploiting the Company’s management tool.”<sup>1</sup> Despite their  
4 contemporaneous knowledge of the massive breaches plaguing Yahoo during the Class Period,  
5 Defendants misled investors through their repeated assurances that “Yahoo! takes your privacy  
6 seriously,” Yahoo has “physical, electronic, and procedural safeguards that comply with federal  
7 regulations to protect [users’] personal information,” “we implemented the latest in security best-  
8 practices,” and “the bad guys who [in the past] have used email spoofing to forge and launch phishing  
9 attempts . . . were nearly stopped in their tracks,” all the while failing to disclose the massive data  
10 breaches threatening the privacy and security of nearly one billion customers.  
11

12  
13 6. Defendants had every reason to keep the breaches under wraps. The concealment  
14 enabled Yahoo to maintain its user base and a needed stream of revenues at a time when the Company’s  
15 financial performance was severely deteriorating. For example, while all online advertising revenue in  
16 the U.S. increased by 16.9% year over year in Q3 2014 to \$12.4 billion, Yahoo’s gross advertising  
17 revenues declined by 1.3% to 4.61 billion. This lackluster performance prompted repeated calls for  
18 Yahoo to sell itself. But even as it was finalizing a sale of its core business to Verizon in 2016, Yahoo  
19 falsely represented in a regulatory filing on September 9, 2016, that “there have not been any incidents  
20 of, or third-party claims alleging, (i) Security Breaches, unauthorized access or unauthorized use of any  
21 of Seller’s or the Business Subsidiaries’ information technology systems or (ii) loss, theft, unauthorized  
22 access or acquisition, modification, disclosure, corruption, or other misuse of any Personal Data” in  
23 Yahoo’s possession. Since the breaches came to light, Verizon has threatened to walk out of the deal.  
24 More recently, Verizon has successfully renegotiated a \$ 350 million price reduction and has required  
25 Yahoo to pay 50% of post-closing cash liabilities related to the data breaches.  
26  
27

28 <sup>1</sup> Unless otherwise stated, all emphases are added.

1 7. Yahoo's silence in the face of a duty to disclose angered not only investors, but U.S.  
2 senators as well, who called the Company's conduct "unacceptable" and questioned its "truthfulness in  
3 representations to the public." When the market learned of the data breaches through a series of  
4 corrective disclosures, Yahoo's shares plummeted by over 31%, significantly harming investors.  
5 Moreover, during the Class Period, Yahoo's core business declined by billions of dollars, leaving  
6 investors exposed to inaccurate assumptions as a result of Defendants' failure to disclose the data  
7 breaches, and inflicting additional harm on investors.  
8

9 8. As a result of its misconduct, Yahoo is the subject of numerous U.S. and foreign  
10 government investigations, including by the SEC, the Federal Trade Commission and other federal,  
11 state, and foreign governmental officials and agencies, including a number of State Attorneys General,  
12 and the U.S. Attorney's office for the Southern District of New York, and is facing no fewer than 43  
13 consumer class actions.  
14

#### 15 **JURISDICTION AND VENUE**

16 9. The claims asserted herein arise under and pursuant to §§10(b) and 20(a) of the  
17 Exchange Act (15 U.S.C. §§78j(b) and 78t(a)) and Rule 10b-5 promulgated thereunder by the SEC (17  
18 C.F.R. §240.10b-5).  
19

20 10. This Court has jurisdiction over the subject matter of this action under 28 U.S.C. §1331  
21 and §27 of the Exchange Act.

22 11. Venue is proper in this Judicial District pursuant to §27 of the Exchange Act (15 U.S.C.  
23 §78aa) and 28 U.S.C. §1391(b). Yahoo's principal executive offices are located within this Judicial  
24 District.  
25

26 12. In connection with the acts, conduct and other wrongs alleged in this Complaint,  
27 Defendants, directly or indirectly, used the means and instrumentalities of interstate commerce,  
28

1 including but not limited to, the United States mail, interstate telephone communications and the  
2 facilities of the national securities exchange.

3 **PARTIES**

4 13. Plaintiffs, as set forth in the Certifications previously filed with the Court, purchased  
5 Yahoo securities at artificially inflated prices during the Class Period and were damaged upon the  
6 revelation of the alleged corrective disclosures.

7  
8 14. Defendant Yahoo! Inc. is incorporated in Delaware, and the Company's principal  
9 executive offices are located at 701 First Avenue, Sunnyvale, California, 94089. Yahoo's common  
10 stock trades on the NASDAQ under the ticker symbol "YHOO."

11 15. Defendant Marissa A. Mayer ("Mayer") has served at all relevant times as the  
12 Company's Chief Executive Officer ("CEO") and a member of the Company's Board of Directors.

13  
14 16. Defendant Ronald S. Bell ("Bell") served as General Counsel and Secretary of Yahoo  
15 from August 13, 2012 until March 1, 2017. Bell served as Vice President at Yahoo from 2001 until  
16 March 1, 2017. He served as Deputy General Counsel of the Americas Region from March 2010 to  
17 July 2012.

18 17. Defendant Alex Stamos ("Stamos") served as Yahoo's Chief Information Security  
19 Officer from March 10, 2014 to approximately June 30, 2015. Stamos reported directly to Defendant  
20 Mayer.

21  
22 18. The Defendants referenced above in ¶¶15-17 are sometimes referred to herein as the  
23 "Individual Defendants."

24 **SUBSTANTIVE ALLEGATIONS**

25 **Background**

26  
27 19. Yahoo, together with its subsidiaries, is a multinational technology company that  
28 provides a variety of internet services, including, *inter alia*, a web portal, search engine, Yahoo! Mail,

1 Yahoo! News, Yahoo! Finance, sports, advertising, and a microblogging and social networking website,  
2 Tumblr. As of February 2016, Yahoo had an estimated 1 billion monthly active users. To utilize  
3 Yahoo's services, users must setup user account(s), which requires users to provide Yahoo with private,  
4 personal information.

5 20. Yahoo derives most of its revenue from advertising through search, display, and native  
6 advertising, including mobile advertising. Critical to Yahoo's appeal to advertisers is their ability to  
7 target advertisements to users based upon their personal information. Yahoo prominently features this  
8 ability to collect information, target specific demographics, and track users' browsing and offline habits  
9 in its pitch to advertisers.  
10

11 21. Accordingly, as part of its business, Yahoo collects and stores large volumes of private  
12 information about its users, including the users' names, email addresses, telephone numbers, birth  
13 dates, passwords, social security numbers, information about assets, and security questions linked to a  
14 user's account ("Private Information"). Yahoo requires this information in order to create an account  
15 and/or for its financial products and services.  
16

17 22. During the Class Period, Yahoo represented that "protecting our systems and our users'  
18 information is paramount to ensuring Yahoo users enjoy a secure user experience and maintaining our  
19 users' trust."<sup>2</sup> Yahoo vouched that "[w]e have physical, electronic, and procedural safeguards that  
20 comply with federal regulations to protect personal information about you."<sup>3</sup>  
21

### 22 **Private Information Is Valuable to Criminals**

23 23. It is well known and the subject of many media reports that Private Information is highly  
24 coveted and a frequent target of hackers. Legitimate organizations and criminals alike recognize the  
25 value of Private Information. Otherwise, they would not aggressively seek or pay for it. For example,  
26

27 <sup>2</sup> Security at Yahoo, Yahoo!, <https://policies.yahoo.com/us/en/yahoo/privacy/topics/security/index.htm>.

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



1 in “one of 2013’s largest breaches [involving a leading software company] . . . not only did hackers  
2 compromise the [card holder data] of three million users, they also took registration data from 38  
3 million users.”<sup>4</sup> Similarly, in the data breach of Target Corporation, between November 27 and  
4 December 15, 2013, hackers stole personal information of as many as 70 million people, including  
5 customer names, mailing addresses, phone numbers, credit or debit card numbers, and the card’s  
6 expiration date and CVV (card verification value). “Increasingly, criminals are using biographical data  
7 gained from multiple sources to perpetrate more and larger thefts.”<sup>5</sup>

8  
9 24. Private Information is “as good as gold” to identity thieves, in the words of the Federal  
10 Trade Commission (“FTC”).<sup>6</sup> Identity theft occurs when someone uses another’s personal identifying  
11 information, such as that person’s name, address, credit card number, credit card expiration date, and  
12 other information, without permission, to commit fraud or other crimes. The FTC estimates that as  
13 many as 10 million Americans have their identities stolen each year. As the FTC recognizes, once  
14 identity thieves have private information, “they can drain your bank account, run up charges on your  
15 credit cards, open new utility accounts, or get medical treatment on your health insurance.”<sup>7</sup>

16  
17 25. According to Javelin Strategy and Research, “1 in 4 data breach notification recipients  
18 became a victim of identity fraud.”<sup>8</sup> Nearly half (46%) of consumers with a breached debit card  
19 became fraud victims within the same year.  
20

21 26. Identity thieves can use Private Information to perpetrate a variety of crimes. For  
22 instance, they may commit various types of fraud upon the U.S. government, such as: immigration

23 <sup>4</sup> Verizon 2014 PCI Compliance Report, [http://www.nocash.info.ro/wp-content/uploads/2014/02/  
24 Verizon\\_pci-report-2014.pdf](http://www.nocash.info.ro/wp-content/uploads/2014/02/Verizon_pci-report-2014.pdf) (hereafter “2014 Verizon Report”), at 54.

25 <sup>5</sup> *Id.*

26 <sup>6</sup> FTC Interactive Toolkit, Fighting Back Against Identity Theft,  
<http://www.dcsheiff.net/community/documents/id-theft-tool-kit.pdf>.

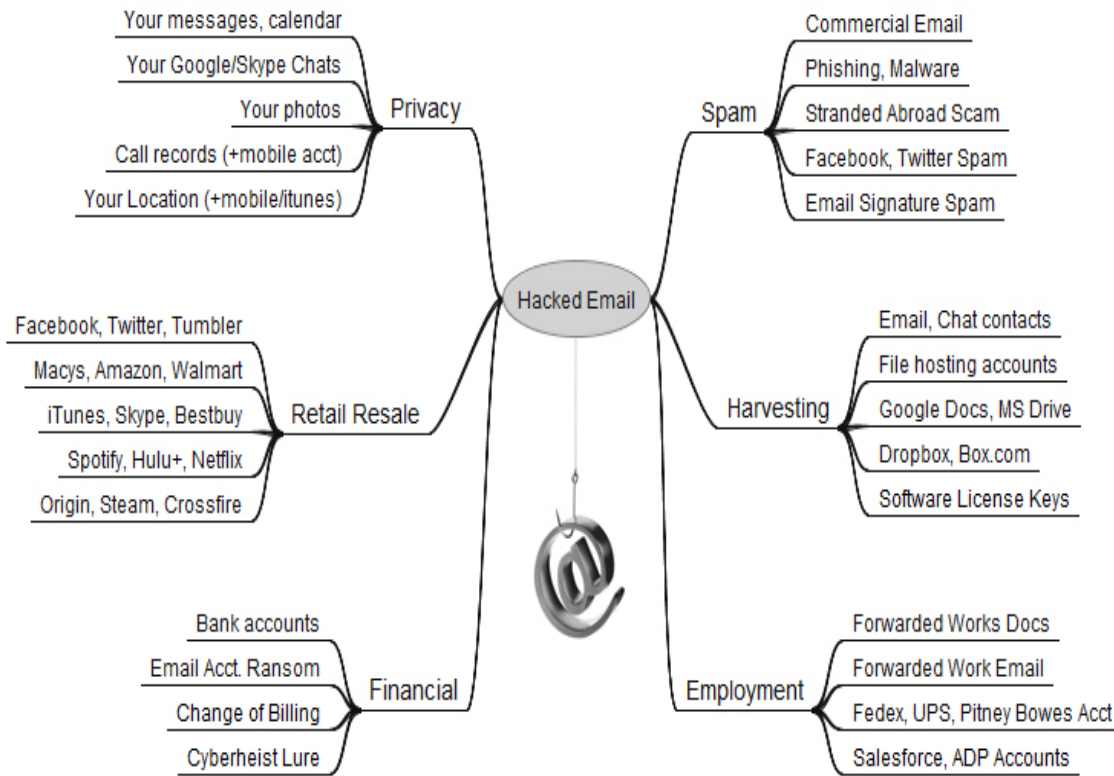
27 <sup>7</sup> FTC, Signs of Identity Theft, available at [http://www.consumer.ftc.gov/articles/0271-signs-identity-  
theft](http://www.consumer.ftc.gov/articles/0271-signs-identity-theft).

28 <sup>8</sup> 2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters,  
<http://www.javelinstrategy.com/brochure/276> (the “2013 Identity Fraud Report”).

1 fraud; obtaining a driver’s license or identification card in the victim’s name but with another’s picture;  
 2 using the victim’s information to obtain government benefits; or filing a fraudulent tax return using the  
 3 victim’s information to obtain a fraudulent refund.

4 27. Additionally, identity thieves may obtain medical services using consumers’  
 5 compromised private information or commit any number of other frauds, such as obtaining a job,  
 6 procuring housing, or even giving false information to police during an arrest.

8 28. As depicted in the chart below, a hacked email account gives criminals access to a  
 9 treasure trove of Private Information:<sup>9</sup>



24 29. According to Steve Grobman, chief technology officer for Intel Security, email accounts  
 25 are a jackpot for criminals, as they often contain passwords for financial and workplace accounts,  
 26 information about investments, and details about the work projects and business plans of anyone from  
 27

28 <sup>9</sup> Brian Krebs, *The Value of a Hacked Email Account*, KrebsOnSecurity (June 13, 2013),  
<http://www.krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account>.

1 an ordinary person to a CEO, lawyer, or military officer. “The public disclosure of such material could  
2 be sensitive enough to destroy careers, enable blackmail, endanger a mission, or influence high-level  
3 negotiations and decisions,” Grobman said.

4 30. The risks associated with data breaches are heightened by the fact that it has become  
5 increasingly common for individuals to use the same passwords for multiple accounts, so the same  
6 password used for a Yahoo account can be used for an online bank account.

7  
8 31. Accordingly, the risks associated with identity theft are grave. “While some identity  
9 theft victims can resolve their problems quickly, others spend hundreds of dollars and many days  
10 repairing damage to their good name and credit record. Some consumers victimized by identity theft  
11 may lose out on job opportunities, or be denied loans for education, housing or cars because of negative  
12 information on their credit reports. In rare cases, they may even be arrested for crimes they did not  
13 commit.”<sup>10</sup>

14  
15 32. A Presidential Report on identity theft from 2008 describes the protracted, harmful  
16 effects of such theft:

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

23 In addition to out-of-pocket expenses that can reach thousands of dollars for the victims  
24 of new account identity theft, and the emotional toll identity theft can take, some victims  
25 have to spend what can be a considerable amount of time to repair the damage caused by  
26 the identity thieves. Victims of new account identity theft, for example, must correct  
27 fraudulent information in their credit reports and monitor their reports for future  
28 inaccuracies, close existing bank accounts and open new ones, and dispute charges with  
individual creditors.<sup>11</sup>

---

<sup>10</sup> True Identity Protection: Identity Theft Overview, <http://www.idwatchdog.com/tikia//pdfs/Identity-Theft-Overview.pdf>.

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

1           33. Annual monetary losses from identity theft are in the billions of dollars. Javelin Strategy  
2 and Research reports that those losses increased to \$21 billion in 2013.<sup>12</sup>

3           34. During the Class Period, Yahoo has repeatedly acknowledged that one of its main  
4 operating risks is that of cybersecurity attacks: “If our security measures are breached, our products and  
5 services may be perceived as not being secure, users and customers may curtail or stop using our  
6 products and services, and we may incur significant and financial exposure.”

7  
8           35. In its Yahoo Security Center, Yahoo itself cautioned users to protect their login  
9 credentials, answering its own question: “Why should I worry about my privacy on the Internet?” by  
10 parading a list of harmful consequences stemming from identity theft:

11           You could be locked out of your online account and be unable to access your e-mail.  
12           But there can be even greater consequences. You could be the victim of identity theft.

13           Once identity thieves have your personal information, the results can be far-reaching,  
14           difficult to rectify, and financially devastating.

15           Armed with your credit card information, fraudsters could charge thousands of dollars to  
16           your account before you ever see a statement from your credit card company. They can  
17           open new credit card accounts in your name.

18           Using your identity, they can open a bank account and write bad checks on that account.  
19           They can authorize electronic transfers in your name, draining your bank account. To  
20           avoid legal action against debts they’ve incurred using your identity, they might even  
21           file for bankruptcy in your name.

22           They can take out a loan, buy a car, and get a driver’s license—all in your name. They  
23           may use your name to get a job or file fraudulent tax returns. And if they’re arrested,  
24           they may give your name to the police and fail to show up for their court date. Then, a  
25           warrant for an arrest is issued—in your name.

### 26           **Yahoo Was Required to Timely and Accurately Disclose All of Its Security Vulnerabilities**

27           36. Understanding the gravity of security data breaches and the disastrous consequences  
28           arising from untimely disclosures of such breaches, Yahoo underscored in its securities filings that  
29           almost every state in the country has passed statutes *making it illegal for any company to improperly*  
30           *delay notifying customers of data breaches*. According to Yahoo’s annual filings, “[m]any states have

31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175  
176  
177  
178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222  
223  
224  
225  
226  
227  
228  
229  
230  
231  
232  
233  
234  
235  
236  
237  
238  
239  
240  
241  
242  
243  
244  
245  
246  
247  
248  
249  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269  
270  
271  
272  
273  
274  
275  
276  
277  
278  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
320  
321  
322  
323  
324  
325  
326  
327  
328  
329  
330  
331  
332  
333  
334  
335  
336  
337  
338  
339  
340  
341  
342  
343  
344  
345  
346  
347  
348  
349  
350  
351  
352  
353  
354  
355  
356  
357  
358  
359  
360  
361  
362  
363  
364  
365  
366  
367  
368  
369  
370  
371  
372  
373  
374  
375  
376  
377  
378  
379  
380  
381  
382  
383  
384  
385  
386  
387  
388  
389  
390  
391  
392  
393  
394  
395  
396  
397  
398  
399  
400  
401  
402  
403  
404  
405  
406  
407  
408  
409  
410  
411  
412  
413  
414  
415  
416  
417  
418  
419  
420  
421  
422  
423  
424  
425  
426  
427  
428  
429  
430  
431  
432  
433  
434  
435  
436  
437  
438  
439  
440  
441  
442  
443  
444  
445  
446  
447  
448  
449  
450  
451  
452  
453  
454  
455  
456  
457  
458  
459  
460  
461  
462  
463  
464  
465  
466  
467  
468  
469  
470  
471  
472  
473  
474  
475  
476  
477  
478  
479  
480  
481  
482  
483  
484  
485  
486  
487  
488  
489  
490  
491  
492  
493  
494  
495  
496  
497  
498  
499  
500  
501  
502  
503  
504  
505  
506  
507  
508  
509  
510  
511  
512  
513  
514  
515  
516  
517  
518  
519  
520  
521  
522  
523  
524  
525  
526  
527  
528  
529  
530  
531  
532  
533  
534  
535  
536  
537  
538  
539  
540  
541  
542  
543  
544  
545  
546  
547  
548  
549  
550  
551  
552  
553  
554  
555  
556  
557  
558  
559  
560  
561  
562  
563  
564  
565  
566  
567  
568  
569  
570  
571  
572  
573  
574  
575  
576  
577  
578  
579  
580  
581  
582  
583  
584  
585  
586  
587  
588  
589  
590  
591  
592  
593  
594  
595  
596  
597  
598  
599  
600  
601  
602  
603  
604  
605  
606  
607  
608  
609  
610  
611  
612  
613  
614  
615  
616  
617  
618  
619  
620  
621  
622  
623  
624  
625  
626  
627  
628  
629  
630  
631  
632  
633  
634  
635  
636  
637  
638  
639  
640  
641  
642  
643  
644  
645  
646  
647  
648  
649  
650  
651  
652  
653  
654  
655  
656  
657  
658  
659  
660  
661  
662  
663  
664  
665  
666  
667  
668  
669  
670  
671  
672  
673  
674  
675  
676  
677  
678  
679  
680  
681  
682  
683  
684  
685  
686  
687  
688  
689  
690  
691  
692  
693  
694  
695  
696  
697  
698  
699  
700  
701  
702  
703  
704  
705  
706  
707  
708  
709  
710  
711  
712  
713  
714  
715  
716  
717  
718  
719  
720  
721  
722  
723  
724  
725  
726  
727  
728  
729  
730  
731  
732  
733  
734  
735  
736  
737  
738  
739  
740  
741  
742  
743  
744  
745  
746  
747  
748  
749  
750  
751  
752  
753  
754  
755  
756  
757  
758  
759  
760  
761  
762  
763  
764  
765  
766  
767  
768  
769  
770  
771  
772  
773  
774  
775  
776  
777  
778  
779  
780  
781  
782  
783  
784  
785  
786  
787  
788  
789  
790  
791  
792  
793  
794  
795  
796  
797  
798  
799  
800  
801  
802  
803  
804  
805  
806  
807  
808  
809  
810  
811  
812  
813  
814  
815  
816  
817  
818  
819  
820  
821  
822  
823  
824  
825  
826  
827  
828  
829  
830  
831  
832  
833  
834  
835  
836  
837  
838  
839  
840  
841  
842  
843  
844  
845  
846  
847  
848  
849  
850  
851  
852  
853  
854  
855  
856  
857  
858  
859  
860  
861  
862  
863  
864  
865  
866  
867  
868  
869  
870  
871  
872  
873  
874  
875  
876  
877  
878  
879  
880  
881  
882  
883  
884  
885  
886  
887  
888  
889  
890  
891  
892  
893  
894  
895  
896  
897  
898  
899  
900  
901  
902  
903  
904  
905  
906  
907  
908  
909  
910  
911  
912  
913  
914  
915  
916  
917  
918  
919  
920  
921  
922  
923  
924  
925  
926  
927  
928  
929  
930  
931  
932  
933  
934  
935  
936  
937  
938  
939  
940  
941  
942  
943  
944  
945  
946  
947  
948  
949  
950  
951  
952  
953  
954  
955  
956  
957  
958  
959  
960  
961  
962  
963  
964  
965  
966  
967  
968  
969  
970  
971  
972  
973  
974  
975  
976  
977  
978  
979  
980  
981  
982  
983  
984  
985  
986  
987  
988  
989  
990  
991  
992  
993  
994  
995  
996  
997  
998  
999  
1000

<sup>12</sup> 2013 Identity Fraud Report.

1 passed laws requiring notification to users where there is a security breach for personal data, such as  
 2 California's Information Practices Act." These laws subject violators to significant damages.

3 37. On its official website, Yahoo represented that:

4 *At Yahoo we take our users' privacy seriously no matter where they are in the world . . .*  
 5 *. One example of this is our close collaboration over the last year with the*  
 6 *Organisation for Economic Cooperation and Development (OECD) as it updated its*  
 7 *Privacy Guidelines . . . These latest privacy guidelines reference new topics including*  
 8 *the strategic importance of national privacy strategies, privacy management programs,*  
 9 *and data breach notification . . . The OECD's Privacy Guidelines are one of the most*  
 10 *commonly referenced privacy frameworks in the world, influencing fair information*  
 11 *practices and privacy fundamentals in . . . the United States . . . Yahoo's Global Public*  
 12 *Policy and Privacy teams will continue to engage in efforts like these to help advance*  
 13 *privacy frameworks that protect our users . . .*

14 38. In connection with these statements, Yahoo provided a direct link on its official website  
 15 to the OECD Privacy Guidelines, which discussed the enactment of laws requiring companies to  
 16 disclose security breaches since "data controllers have little incentive to disclose breaches voluntarily":

17 The potential harm to individuals from the misuse of their personal data, whether  
 18 accidentally lost or purposefully stolen, may be significant.

19 *Organisations experiencing a breach often incur significant costs responding to it,*  
 20 *determining its cause, and implementing measures to prevent recurrence. The*  
 21 *reputational impact can also be significant. A loss of trust or confidence can have*  
 22 *serious consequences for organisations. As a result, the security of personal data has*  
 23 *become an issue of great concern to governments, businesses and individuals.*

24 *Breach notification laws requiring data controllers to inform individuals and/or*  
 25 *authorities when a security breach has occurred have been passed or proposed in many*  
 26 *countries. These laws are usually justified on the grounds that data controllers have*  
 27 *little incentive to disclose breaches voluntarily, given the possible harm this can cause*  
 28 *to their reputation.* Requiring notification may enable individuals to take measures to  
 protect themselves against the consequences of identity theft or other harms.

Notification requirements may also provide privacy enforcement authorities or other  
 authorities with information to determine whether to investigate the incident or take  
 other action. Ideally, breach notification laws also help to create an incentive for data  
 controllers to adopt appropriate security safeguards for the personal data they hold.

\* \* \*

Furthermore, mandatory security breach notification may improve the evidence base for  
 privacy and information security policies by generating information about the number,  
 severity and causes of security breaches.

1 Security breaches not only raise privacy concerns, but also intersect with other issues,  
 2 including criminal law enforcement and cybersecurity. When an organisation suffers a  
 3 security breach, particularly one resulting from an external attack, notification of the  
 4 breach to authorities other than privacy enforcement authorities (e.g. computer incident  
 response teams, criminal law enforcement entities, other entities responsible for  
 cybersecurity oversight) may be appropriate or required.

5 Requiring notification for every data security breach, no matter how minor, may impose  
 6 an undue burden on data controllers and enforcement authorities, for limited  
 7 corresponding benefit. Additionally, excessive notification to data subjects may cause  
 8 them to disregard notices. Accordingly, the new provision that has been added to the  
 9 Guidelines [paragraph 15(c)] reflects a risk-based approach to notification. *Notice to an  
 authority is called for where there is a “significant security breach affecting personal  
 data,” a concept intended to capture a breach that puts privacy and individual liberties  
 at risk. Where such a breach is also likely to adversely affect individuals, notification  
 to individuals would be appropriate as well.*

10 39. Yahoo also represented on its website that it *will notify users “if we strongly suspect  
 11 that your account may have been targeted by a state-sponsored actor.* We’ll provide these specific  
 12 notifications so that our users can take appropriate measures to protect their accounts and devices in  
 13 light of these sophisticated attacks.”

14 40. Additionally, as early as October 2011, the SEC has issued guidelines regarding  
 15 disclosure obligations of filers relating to cybersecurity risks and cyber incidents, in light of the  
 16 frequent and severe nature of cyber incidents.<sup>13</sup> The SEC emphasized that “the federal securities laws,  
 17 in part, are designed to elicit disclosure of *timely, comprehensive, and accurate information* about  
 18 risks and events that a reasonable investor would consider important to an investment decision”:  
 19

20 [M]aterial information regarding cybersecurity risks and cyber incidents is required to be  
 21 disclosed when necessary in order to make other required disclosures, in light of the  
 22 circumstances under which they are made, not misleading.

### 23 **Risk Factors**

24 Registrants should disclose the risk of cyber incidents *if these issues are among the  
 25 most significant factors that make an investment in the company speculative or risky.*  
 26 In determining whether risk factor disclosure is required, we expect registrants to  
 27 evaluate their cybersecurity risks and take into account all available relevant  
 information, including prior cyber incidents and the severity and frequency of those

28 <sup>13</sup> See <http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm>.

1 incidents. As part of this evaluation, registrants should consider the probability of cyber  
 2 incidents occurring ***and the quantitative and qualitative magnitude of those risks,***  
 3 ***including the potential costs and other consequences resulting from misappropriation***  
 4 ***of assets or sensitive information, corruption of data or operational disruption.*** In  
 5 evaluating whether risk factor disclosure should be provided, registrants should also  
 6 consider the adequacy of preventative actions taken to reduce cybersecurity risks in the  
 7 context of the industry in which they operate and risks to that security, including  
 8 threatened attacks of which they are aware.

9 Consistent with the Regulation S-K Item 503(c) requirements for risk factor disclosures  
 10 generally, cybersecurity risk disclosure provided must adequately describe the nature of  
 11 the material risks and specify how each risk affects the registrant. Registrants should not  
 12 present risks that could apply to any issuer or any offering and should avoid generic risk  
 13 factor disclosure. Depending on the registrant's particular facts and circumstances, and  
 14 to the extent material, appropriate disclosures may include . . .

- 15 • Description of cyber incidents experienced by the registrant that are individually,  
 16 or in the aggregate, material, including a description of the costs and other  
 17 consequences;
- 18 • Risks related to cyber incidents that may remain undetected for an extended  
 19 period . . .

20 A registrant may need to disclose known or threatened cyber incidents to place the  
 21 discussion of cybersecurity risks in context. ***For example, if a registrant experienced a***  
 22 ***material cyber attack in which malware was embedded in its systems and customer***  
 23 ***data was compromised, it likely would not be sufficient for the registrant to disclose***  
 24 ***that there is a risk that such an attack may occur.*** Instead, as part of a broader  
 25 discussion of malware or other similar attacks that pose a particular risk, ***the registrant***  
 26 ***may need to discuss the occurrence of the specific attack and its known and potential***  
 27 ***costs and other consequences.***<sup>14</sup>

28 41. The SEC explained that “[i]nformation is considered material if there is a substantial  
 likelihood that a reasonable investor would consider it important in making an investment decision or if  
 the information would significantly alter the total mix of information made available. See *Basic Inc. v.*  
*Levinson*, 485 U.S. 224 (1988); and *TSC Industries, Inc. v. Northway, Inc.*, 426 U.S. 438 (1976).  
 Registrants also should consider the antifraud provisions of the federal securities laws, which apply to  
 statements and omissions both inside and outside of Commission filings. See Securities Act Section  
 17(a); Exchange Act Section 10(b); and Exchange Act Rule 10b-5.”<sup>15</sup>

<sup>14</sup> *Id.*

<sup>15</sup> *Id.*

1           42.     The SEC also requires public companies to report material events on a current basis.  
2 Form 8-K is the “current report” companies must file with the SEC to announce major events that  
3 shareholders should know about.

4           43.     In addition to the SEC’s specific requirements regarding cybersecurity disclosures  
5 described above, in June 2014, SEC Commissioner Luis A. Aguilar provided further guidance to  
6 companies regarding cybersecurity incidents and the need for their disclosure:  
7

8           In addition to becoming more frequent, there are reports indicating that cyber-attacks  
9 have become increasingly costly to companies that are attacked. According to one 2013  
10 survey, the average annualized cost of cyber-crime to a sample of U.S. companies was  
11 \$11.6 million per year, representing a 78% increase since 2009. In addition, the  
12 aftermath of the 2013 Target data breach demonstrates that the impact of cyber-attacks  
13 may extend far beyond the direct costs associated with the immediate response to an  
14 attack. *Beyond the unacceptable damage to consumers, these secondary effects  
include reputational harm that significantly affects a company’s bottom line. In sum,  
the capital markets and their critical participants, including public companies, are  
under a continuous and serious threat of cyber-attack, and this threat cannot be  
ignored.*

15           *As an SEC Commissioner, the threats are a particular concern because of the  
widespread and severe impact that cyber-attacks could have on the integrity of the  
capital markets infrastructure and on public companies and investors. The concern is  
not new.* For example, in 2011, staff in the SEC’s Division of Corporation Finance  
16 issued guidance to public companies regarding their disclosure obligations with respect  
17 to cybersecurity risks and cyber-incidents. More recently, because of the escalation of  
18 cyber-attacks, I helped organize the Commission’s March 26, 2014 roundtable to discuss  
19 the cyber-risks facing public companies and critical market participants like exchanges,  
20 broker-dealers, and transfer agents.

21           As it has been noted, the primary distinction between a cyber-attack and other crises that  
22 a company may face is the speed with which the company must respond to contain the  
23 rapid spread of damage. *Companies need to be prepared to respond within hours, if  
not minutes, of a cyber-event to detect the cyber-event, analyze the event, prevent  
further damage from being done, and prepare a response to the event.*

24           While there is no “one-size-fits-all” way to properly prepare for the various ways a  
25 cyber-attack can unfold, and what responses may be appropriate, it can be just as  
26 damaging to have a poorly-implemented response to a cyber-event. As others have  
27 observed, an “ill-thought-out response can be far more damaging than the attack itself.”  
Accordingly, *boards should put time and resources into making sure that management  
has developed a well-constructed and deliberate response plan that is consistent with  
best practices for a company in the same industry.*

28           *These plans should include, among other things, whether, and how, the cyber-attack  
will need to be disclosed internally and externally (both to customers and to investors).*



1 In deciding the nature and extent of the disclosures, *I would encourage companies to go*  
2 *beyond the impact on the company and to also consider the impact on others. It is*  
3 *possible that a cyber-attack may not have a direct material adverse impact on the*  
4 *company itself, but that a loss of customers' personal and financial data could have*  
5 *devastating effects on the lives of the company's customers and many Americans. In*  
6 *such cases, the right thing to do is to give these victims a heads-up so that they can*  
7 *protect themselves.*

8 [B]oard oversight of cyber-risk management is critical to ensuring that companies are  
9 taking adequate steps to prevent, and prepare for, the harms that can result from such  
10 attacks. There is no substitution for proper preparation, deliberation, and engagement on  
11 cybersecurity issues. *Given the heightened awareness of these rapidly evolving risks,*  
12 *directors should take seriously their obligation to make sure that companies are*  
13 *appropriately addressing those risks.*

14 44. Under Yahoo's own Vulnerability Disclosure Policy in place during the Class Period,  
15 which the Company posted on its official website, Yahoo vouched to publicly disclose all security  
16 vulnerabilities within 90 days of discovery:

17 *Time is of the essence when we discover these types of issues: the more quickly we*  
18 *address the risks, the less harm an attack can cause. Today, we are committing to*  
19 *publicly disclosing on our security Tumblr the vulnerabilities we discover within 90*  
20 *days. By committing to this short time frame, we will help ensure that these*  
21 *vulnerabilities are patched as quickly as possible.*

22 45. Yahoo's Vulnerability Disclosure Policy included a section on Frequently Asked  
23 Questions:

24 Q: Why does Yahoo disclose security vulnerabilities?

25 A: Disclosing security vulnerabilities allows everyone to patch their systems. We have to  
26 assume that 3rd parties are already aware of these issues or may become aware soon.  
27 There is solid evidence that attackers commonly discover and exploit 0-day  
28 vulnerabilities all the time.

Q: Why 90 days? Why not 15 or 120?

A: We feel 90 days is a long enough timeline that developers can write, test and deploy a  
fix to an issue. Within this time we will do our best to coordinate disclosure of the  
vulnerability and ensure that a proper fix has been developed. Furthermore, we hold  
ourselves to the same standard (<http://hackerone.com/yahoo>) and expect our own  
developers to fix security issues within 90 days. We anticipate many security issues will  
be fixed and patches deployed well before the 90 day timeline has expired.

Q: What happens after 90 days?

1 A: This depends on the current state of a fix for the vulnerability. If we are in good  
 2 contact with the party responsible for developing and deploying a fix but they need more  
 3 time then we reserve the right to extend this deadline as necessary. If we feel no progress  
 4 is being made on the fix then we reserve the right to publish the vulnerability details so  
 5 that the internet community is aware of the issue and individual organizations can defend  
 6 against or patch it themselves. When this occurs we will do our best to provide  
 7 mitigation guidance where appropriate. We will make every effort possible to contact all  
 8 relevant parties and help to coordinate the disclosure when needed.

6 Q: Is Yahoo actively looking for vulnerabilities in open and closed source software?

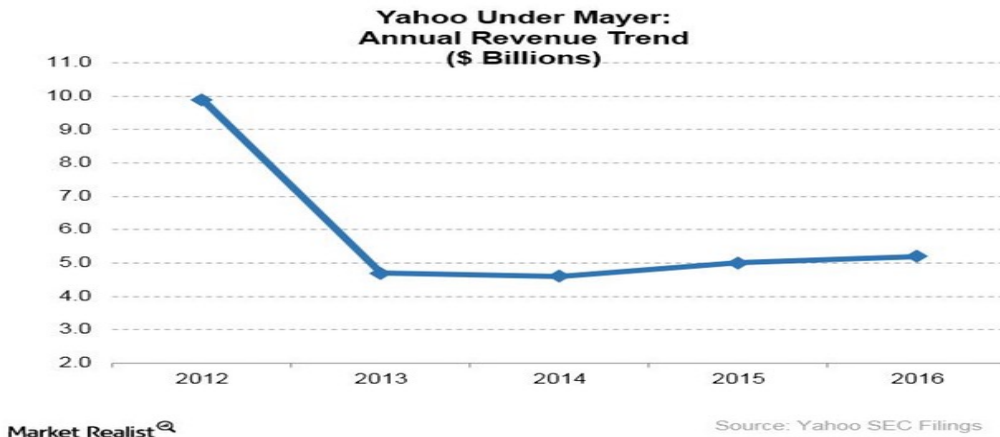
7 A: Yes. Part of our job is to always be on the lookout for security vulnerabilities that  
 8 affect the technologies that Yahoo uses and this includes software we didn't develop at  
 9 Yahoo. These efforts are part of our larger commitment to user security, safety and  
 10 privacy.

10 Q: Is Yahoo hoarding 0-day [previously unknown security] vulnerabilities?

11 A: Never! We disclose all vulnerabilities that we discover according to our policy  
 12 guidelines.

13 **During the Class Period, Yahoo Struggled to Stay Afloat**

14 46. As measured by annual revenue growth, Defendant Mayer's tenure as Yahoo's CEO was  
 15 abysmal:<sup>16</sup>



24 47. In 2015, Yahoo's stock went from a high of \$50.23 in January to a low of \$27.60 in  
 25 September, a 45% price decline.  
 26

28 <sup>16</sup> See <http://www.nytimes.com/2016/09/29/technology/yahoo-data-breach-hacking.html>

1 48. During the Class Period, Yahoo's stock underperformed the markets. For example, the  
2 Company's stock declined by over 17% in the first five months of 2015, while the return on NASDAQ  
3 composite index was close to 7%. One of the reasons behind Yahoo's lackluster performance was the  
4 inability of its core business to deliver the necessary revenue growth from online ads. While online  
5 advertising revenue in the U.S. rose by 16.9% year over year in Q3 2014 to \$12.4 billion, Yahoo's  
6 gross ad revenues declined by 1.3% to 4.61 billion, according to reports by the Interactive Advertising  
7 Bureau and PricewaterhouseCoopers US.  
8

9 49. Also during the Class Period, Yahoo's core business declined by billions of dollars. As  
10 a result of Defendants' failure to disclose the data breaches, during the Class Period investors were  
11 exposed to inaccurate assumptions related to Yahoo's core business, and suffered additional harm.  
12

13 50. Yahoo's deteriorating performance sparked stinging criticism and calls for action from  
14 some of its largest shareholders. For example, on September 26, 2014, investment management firm  
15 Starboard Value LP ("Starboard"), which held a significant ownership stake in Yahoo, demanded that  
16 Defendant Mayer and Yahoo's Board of Directors halt the Company's aggressive acquisition strategy,  
17 which "has resulted in \$1.3 billion of capital spent since Q2 2012 while consolidated revenues have  
18 remained stagnant and EBITDA has materially decreased."<sup>17</sup> Starboard protested that "since new  
19 management was appointed in Q2 2012, revenue in Yahoo's core Search and Display businesses has  
20 been stagnant, yet SG&A and R&D expenditures have grown by a staggering \$390 million, in turn,  
21 causing EBITDA to decline by 19%".<sup>18</sup>  
22  
23  
24  
25  
26

27 <sup>17</sup> See <http://www.prnewswire.com/news-releases/starboard-delivers-letter-to-ceo-and-board-of-directors-of-yahoo-inc-277223182.html>.

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

**Yahoo!'s Core Business performance since Q2 2012:**

\$ in millions

Amount spent in acquisitions since Q2 2012 (\$ in millions)

\$ 1,275

	Q2 2012	Q2 2014	Change	% Change
LTM Sales ex-Traffic Acquisition Costs	\$ 4,399	\$ 4,408	\$ 9	0%
LTM EBITDA <sup>(1)(2)</sup>	\$ 1,629	\$ 1,314	\$ (315)	(19)%
Stock-Based Compensation Expense	\$ 199	\$ 377	\$ 178	90%
LTM SG&A and R&D Excluding Amortization	\$ 2,534	\$ 2,920	\$ 386	15%

Source: Company Filings and Presentations, Starboard Research

51. Starboard assailed Yahoo for recklessly spending \$1.3 billion on acquisitions that failed to deliver shareholder value and were instead money-losing businesses. According to Starboard, “[o]ur analysis indicates that Yahoo's display business, where management's efforts and acquisitions have been focused, may be losing over \$500 million in EBITDA per year”:<sup>19</sup>

**Yahoo! 2014 Segment Profitability Estimates**

\$ in millions

	Revenue	Opex	EBITDA
Search	\$ 1,780	\$ (534)	\$ 1,246
Display	1,600	(2,152)	(552)
Other: Listing, Transaction, and Fees (Excl. Royalties, and TIPLA amort.)	343	(206)	137
Alibaba Royalty	86	-	86
Yahoo Japan Royalty	264	-	264
<b>Consolidated</b>	<b>\$ 4,073</b>	<b>\$ (2,892)</b>	<b>\$ 1,182</b>

Source: Starboard Research and Estimates

52. Calling Yahoo’s financial performance “unacceptable,” Starboard urged the Company to explore “a strategic combination” with AOL in order to unleash synergies and revive profitability in its highly trafficked digital properties.<sup>20</sup>

53. In early 2016, Yahoo continued to experience a sharp decline in both revenues and earnings compared to 2015, with revenue falling nearly 15% and earnings over 20%. Analysts warned that the Company’s condition was becoming “increasingly dire.” By the end of 2016, Yahoo expected to have a workforce 42% smaller than it was in 2012, when Defendant Mayer took office.

54. Analysts have called Mayer’s performance during the Class Period “awful,” observing that under her leadership Yahoo was “massively underperforming its potential and [was] struggling to hold onto its executives.”<sup>21</sup>

<sup>19</sup> *Id.*<sup>20</sup> *Id.*

1 55. Bowing to pressure from investors unhappy with the eroding financial performance  
2 under Mayer's leadership—including the \$4.46 goodwill impairment charge taken in 2015 and the  
3 hundreds of millions in stock options awarded in 2015 alone—in February 2016, Yahoo officially put  
4 itself up for sale. Reportedly, Yahoo gave potential bidders until April 18, 2016 to place their bids.  
5 Bidders at the time included Daily Mail, Time Inc., Google, Microsoft, Verizon, and private equity  
6 firms General Atlantic, TPG and KKR. If Yahoo did not sell itself, analysts said it could begin “a nasty  
7 battle” with Starboard, which threatened to nominate an entirely new slate of directors at Yahoo's next  
8 shareholder meeting.  
9

10 56. On or around June 9, 2016, Yahoo received a second round of multiple bids, with  
11 Verizon bidding more than \$3.5 billion. Other bidders included AT&T, TPG, and a consortium  
12 including Bain Capital, Vista Equity Partners, and Ross Levinsohn. Yahoo's Board of Directors was  
13 scheduled to review the second round of bids on June 10, 2016. The final round of the sales process  
14 was expected to conclude in mid-July 2016.  
15

16 57. On July 23, 2016, Yahoo entered into a Stock Purchase Agreement (“2016 Agreement”)  
17 with Verizon, the winning bidder, pursuant to which Verizon would purchase the core business of  
18 Yahoo for a consideration of approximately \$4.8 billion in cash. Verizon planned to integrate Yahoo's  
19 core business with AOL, the iconic web brand that Verizon bought in 2015 for \$4.4 billion in a push to  
20 create a digital media operation to supplement the company's dominant cable and wireless business. At  
21 the time, Yahoo announced that the transaction with Verizon was not expected to close until the first  
22 quarter of 2017.  
23

24 58. Pursuant to the terms of the 2016 Agreement, the sale to Verizon includes all assets and  
25 liabilities of Yahoo's operating business, including Yahoo's products, brands, worldwide offices and  
26 business operations, other than a few assets and liabilities identified as Excluded Assets or Retained  
27

28 <sup>21</sup> *Yahoo 'Underperforming' Big-Time, Analyst Says*, Investor's Business Daily, Dec. 10, 2015.

1 Liabilities. The Excluded Assets and Retained Liabilities include: all shares in Alibaba Group Holding;  
2 all shares in Yahoo Japan, other than commercial arrangements with Yahoo Japan; Yahoo's non-core  
3 IP, known as the Excalibur IP portfolio; certain minority investment interests; cash at closing; and  
4 Yahoo's outstanding convertible notes and certain other retained liabilities. Under the 2016  
5 Agreement, Verizon assumed all liability arising from Yahoo's core, operating business, including  
6 liabilities "arising from or related to any period prior to" closing of the transaction. With respect to  
7 management changes, Yahoo announced that "Verizon and Yahoo will discuss potential integration  
8 plans (including reporting structure) between now and closing" and that "post-closing Verizon will  
9 determine the leadership structure of the combined entity."

11 59. Defendant Mayer touted the sale as a significant accomplishment for Yahoo: "The sale  
12 of our operating business, which effectively separates our Asian asset equity stakes, is an important step  
13 in our plan to unlock shareholder value for Yahoo. This transaction also sets up a great opportunity for  
14 Yahoo to build further distribution and accelerate our work in mobile, video, native advertising and  
15 social."

17 60. Verizon's Chairman and CEO, Lowell McAdam, also praised the deal as an achievement  
18 by Verizon in obtaining Yahoo's "global audience of more than 1 billion monthly active users—  
19 including 600 million monthly active mobile users": "Just over a year ago we acquired AOL to  
20 enhance our strategy of providing a cross-screen connection for consumers, creators and advertisers.  
21 The acquisition of Yahoo will put Verizon in a highly competitive position as a top global mobile  
22 media company, and help accelerate our revenue stream in digital advertising."

24 61. As explained in detail below, by intentionally hiding from investors the massive data  
25 breaches that plagued it during the Class Period, the Company was able to attract and maintain users  
26 who were duped into believing that Yahoo's services were secure, thus providing the Company with a  
27 continuing stream of revenue. This revenue stream was critical for Yahoo at a time when it was  
28

1 struggling amid intense competition. By concealing the data breaches from the public, Yahoo also  
2 found a suitor willing to acquire its operating business.

3 **Despite Being Repeatedly Hacked During the Class Period,**  
4 **Yahoo Refused to Invest in Needed Security Upgrades**

5 62. Yahoo is no stranger to threats against its users' Private Information. On July 11, 2012,  
6 over 450,000 unencrypted Yahoo usernames and passwords were stolen and posted on a public  
7 website.<sup>22</sup>

8 63. Yahoo disclosed that breach promptly—the following day.

9 64. In that breach, the hackers used a technique known as a “SQL injection attack,” which  
10 works by “injecting” malicious commands into the stream of commands between a website application  
11 and the database software feeding it. In essence, a SQL injection attack exploits the way in which a  
12 website communicates with back-end databases, allowing an attacker to issue commands (in the form of  
13 specially crafted SQL statements) to a database that contains information used by the website  
14 application, such as users' login credentials.  
15

16 65. Yahoo failed to employ basic security measures to protect the stolen information.  
17 Reasonable security measures to protect Private Information would have included securing the data  
18 server containing that information from SQL injection attacks, encrypting critical data (such as login  
19 credentials) contained in the database, and monitoring network activity to identify suspicious amounts  
20 of out-bound data. Proper encryption often includes salting and hashing passwords, which refers to  
21 adding strings of random characters to the passwords and then obscuring the data with a cryptography  
22 algorithm.  
23  
24

25  
26  
27 <sup>22</sup> See, e.g., Charles Arthur, *Yahoo Voice Hack Leaks 450,000 Passwords*, The Guardian (July 12,  
28 2012), <https://www.theguardian.com/technology/2012/jul/12/yahoo-voice-hack-attack-passwords-stolen>;  
Chenda Ngak, *Yahoo Confirms Email Hack In Statement*, CBS News (July 12, 2012),  
<http://www.cbsnews.com/news/yahoo-confirms-email-hack-in-statement>.

1 66. Yahoo's servers should not have been vulnerable to a SQL injection attack. This type of  
 2 injection has been known for over a decade and had already been blamed for massive data thefts against  
 3 Heartland Payment System and others. As far back as 2003, the FTC considered SQL injection attacks  
 4 to be well-known and foreseeable events that could have and should have been taken into account  
 5 through routine security measures, which Yahoo failed to adopt.

6 67. Indeed, "[s]ecurity experts were befuddled . . . as to why a company as large as Yahoo  
 7 would fail to cryptographically store the passwords in its database. Instead, they were left in plain text,  
 8 which means a hacker could easily read them."<sup>23</sup> According to a security researcher at Rapid7,  
 9 Yahoo's security was "definitely poor."<sup>24</sup>

10 68. The hackers perpetrating the 2012 breach warned Yahoo that the hack served as a "*wake*  
 11 *up call*" to spring into action:  
 12

13 We hope that the parties responsible for managing the security of this subdomain will  
 14 take this as a wake-up call, and not as a threat ... There have been many security holes  
 15 exploited in Web servers belonging to Yahoo! Inc. that have caused far greater damage  
 16 than our disclosure. Please do not take them lightly.<sup>25</sup>

17 69. On or around May 17, 2013, Yahoo Japan was compromised, exposing 22 million  
 18 Yahoo Japan email addresses.<sup>26</sup> The Company disclosed the breach three days later, asking more than  
 19 200 million customers to reset their passwords after detecting an intrusion in one of its main servers. In  
 20 a press release published on Yahoo Japan's website, Yahoo stressed that it had not confirmed that the  
 21 data had definitely leaked outside the Company.

22 <sup>23</sup> Antone Gonsalves, *Yahoo security breach shocks experts*, CSO (July 12, 2012),  
 23 [http://www.csoonline.com/article/2131970/identity-theft-prevention/yahoo-security-breach-](http://www.csoonline.com/article/2131970/identity-theft-prevention/yahoo-security-breach-shocksexperts.html)  
 24 [shocksexperts.html](http://www.csoonline.com/article/2131970/identity-theft-prevention/yahoo-security-breach-shocksexperts.html).

24 <sup>24</sup> *Id.*

25 <sup>25</sup> Doug Gross, *Yahoo hacked, 450,000 passwords posted online*, CNN (July 13, 2012, 9:31 AM),  
 26 <http://www.cnn.com/2012/07/12/tech/web/yahoo-users-hacked/>.

27 <sup>26</sup> Graham Cluley, *22 Million User Ids May Be In The Hands Of Hackers, After Yahoo Japan Security*  
 28 *Breach*, NAKED SECURITY (May 20, 2013), <http://www.nakedsecurity.sophos.com/2013/05/20/yahoo-japan-hack/>; BBC Technology, *Millions Hit*  
*By Yahoo Japan Hack Attack*, BBC (May 20, 2013), [http://www.bbc.com/news/technology-](http://www.bbc.com/news/technology-22594136)  
[22594136](http://www.bbc.com/news/technology-22594136).



1 70. Yahoo's utter failure to take even the most rudimentary security steps also enabled  
2 hackers in late December 2013 to target Java in Yahoo's ad network, infecting roughly 27,000  
3 computers per hour at the time of discovery.<sup>27</sup> Critically, Yahoo's failure also enabled the three  
4 massive data breaches that are at the crux of this action: the 2013 Data Breach, the 2014 Data Breach,  
5 and the Forged Cookie Data Breach (described below)—the first two widely regarded as *the biggest*  
6 *data breaches in U.S. history*.

7  
8 71. The technology industry is rife with similar examples of hackers targeting users' Private  
9 Information, including the hacks at Adobe,<sup>28</sup> LinkedIn, eHarmony,<sup>29</sup> and Snapchat,<sup>30</sup> among many  
10 others, all of which pre-date the timeframe Yahoo has identified regarding the 2014 Data Breach, and  
11 some of which pre-date the 2013 Data Breach. As a company in the online services arena, which  
12 employs security professionals, Yahoo undoubtedly knew about these hacks and the high probability  
13 that it could suffer similar hacks.

14  
15 72. Despite experiencing the significant data breaches described above, Yahoo knowingly  
16 continued to utilize outdated security methods. As reported by Reuters on December 18, 2016, at the  
17 time of the 2013 Data Breach, Yahoo used an encryption protocol called MD5 that was considered  
18 inadequate by online security professionals. Indeed, a public warning was issued about the inadequacy  
19 of MD5 as early as 2008:<sup>31</sup>

20  
21 In 2008, five years before Yahoo took action, Carnegie Mellon University's Software  
22 Engineering Institute issued a public warning to security professionals through a U.S.

23  
24 <sup>27</sup> Andrew Scurria, *European Yahoo Users Victimized In Malware Attack*, Law360 (Jan. 6, 2014),  
<http://www.law360.com/articles/498914>.

25 <sup>28</sup> See *In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197 (N.D. Cal. 2014).

26 <sup>29</sup> CBS News Staff, *eHarmony Suffers Password Breach on Heels of LinkedIn*, CBS News (June 7,  
2012), <http://www.cbsnews.com/news/eharmony-suffers-password-breach-on-heels-of-linkedin>.

27 <sup>30</sup> Nancy Blair & Brett Molina, *Snapchat, Skype Have Security Breach*, USA Today (Jan. 2, 2014),  
<http://www.usatoday.com/story/tech/2014/01/01/snapchat-user-names-leak/4277789>.

28 <sup>31</sup> *Yahoo security problems a story of too little, too late*, Reuters (December 18, 2016),  
<http://www.reuters.com/article/us-yahoo-cyber-insight-idUSKBN1470WT>.

1 government-funded vulnerability alert system: MD5 *“should be considered*  
2 *cryptographically broken and unsuitable for further use.”*

3 Yahoo’s failure to move away from MD5 in a timely fashion was an example of  
4 problems in Yahoo’s security operations as it grappled with business challenges,  
5 according to five former employees and some outside security experts. Stronger hashing  
6 technology would have made it more difficult for the hackers to get into customer  
7 accounts after breaching Yahoo’s network, making the attack far less damaging, they  
8 said.

9 “MD5 was considered dead long before 2013,” said David Kennedy, chief executive of  
10 cyber firm TrustedSec LLC. “Most companies were using more secure hashing  
11 algorithms by then.”

12 He did not name specific firms.

13 73. Brian Krebs, a leading data security researcher discussing the 2013 Data Breach,  
14 concluded that “even by 2013 anyone with half a clue in securing passwords already long knew that  
15 storing passwords in MD5 format was no longer acceptable and [an] altogether braindead idea.”

16 74. As reported by Reuters, former Yahoo security personnel with knowledge of the  
17 Company’s security protocols told Reuters that *“the security team was at times turned down when it*  
18 *requested new tools and features such as strengthened cryptography protections, on the grounds that*  
19 *the requests would cost too much money, were too complicated, or were simply too low a priority.”*<sup>32</sup>

20 According to these former Yahoo employees and to outside security experts, “Yahoo’s failure to move  
21 away from MD5 in a timely fashion was an example of problems in Yahoo’s security operations as it  
22 grappled with business challenges.”<sup>33</sup> “Stronger hashing technology would have made it more difficult  
23 for the hackers to get into customer accounts after breaching Yahoo’s network, making the attack far  
24 less damaging.”<sup>34</sup> Yahoo’s skimping on security reflected the Company’s financial struggles, with  
25

26 <sup>32</sup> *Yahoo seen cutting cost corners with security tech discredited long before massive hack*, Reuters,  
27 Dec. 19, 2016.

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

<sup>34</sup> *Id.*

1 revenues steadily falling since their 2008 peak and Yahoo losing its market dominance to its  
2 competitors, such as Alphabet Inc.’s Google and Facebook.<sup>35</sup>

3 75. The former Yahoo employees said “the Company’s security problems began before the  
4 arrival of Chief Executive Marissa Mayer in 2012 and continued under her tenure. *Yahoo had suffered*  
5 *attacks by Russian hackers for years, two of the former staffers said.*”<sup>36</sup>

6 76. According to a September 28, 2016 New York Times article based on interviews with  
7 several Yahoo insiders who participated in security discussions at Yahoo, “defending against hackers  
8 took a back seat at Yahoo.” According to those insiders, *despite knowing during the Class Period that*  
9 *Yahoo was a frequent target for nation-state spies, Defendant Mayer rejected even the most basic*  
10 *security measures and frequently clashed with Yahoo’s Chief Information Security Officer “for fear*  
11 *that even something as simple as a password change would drive Yahoo’s shrinking email users to*  
12 *other services*”.<sup>37</sup>

13  
14  
15 Six years ago, Yahoo’s computer systems and customer email accounts were penetrated  
16 by Chinese military hackers. Google and a number of other technology companies were  
17 also hit.

18 \* \* \*

19 While Google’s response was public, Yahoo never publicly admitted that it had also  
20 been attacked.

21 \* \* \*

22 The Google co-founder Sergey Brin regarded the attack on his company’s systems as a  
23 personal affront and responded by making security a top corporate priority. Google hired  
24 hundreds of security engineers with six-figure signing bonuses, invested hundreds of  
25 millions of dollars in security infrastructure and adopted a new internal motto, “Never  
26 again,” to signal that it would never again allow anyone—be they spies or criminals—to  
27 hack into Google customers’ accounts.

28 *Yahoo, on the other hand, was slower to invest in the kinds of defenses necessary to*  
*thwart sophisticated hackers that are now considered standard in Silicon Valley,*

---

35 *Id.*

36 *Id.*

37 See <http://www.nytimes.com/2016/09/29/technology/yahoo-data-breach-hacking.html>.

1 *according to half a dozen current and former company employees who participated in*  
2 *security discussions but agreed to describe them only on the condition of anonymity.*

3 *When Marissa Mayer took over as chief executive of the flailing company in mid-*  
4 *2012, security was one of many problems she inherited. With so many competing*  
5 *priorities, she emphasized creating a cleaner look for services like Yahoo Mail and*  
6 *developing new products over making security improvements, the Yahoo employees*  
7 *said.*

8 *The “Paranoids,” the internal name for Yahoo’s security team, often clashed with*  
9 *other parts of the business over security costs. And their requests were often*  
10 *overridden because of concerns that the inconvenience of added protection would*  
11 *make people stop using the company’s products.*

12 \* \* \*

13 But Yahoo’s choices had consequences, resulting in a series of embarrassing security  
14 failures over the last four years. . . .

15 \* \* \*

16 *To make computer systems more secure, a company often has to make its products*  
17 *slower and more difficult to use. It was a trade-off Yahoo’s leadership was often*  
18 *unwilling to make.*

19 \* \* \*

20 *In 2013, disclosures by Edward J. Snowden, the former National Security Agency*  
21 *contractor, showed that Yahoo was a frequent target for nation-state spies.* Yet it took  
22 a full year after Mr. Snowden’s initial disclosures for Yahoo to hire a new chief  
23 information security officer, Alex Stamos.

24 Jeff Bonforte, the Yahoo senior vice president who oversees its email and messaging  
25 services, said in an interview last December that Mr. Stamos and his team had pressed  
26 for Yahoo to adopt end-to-end encryption for everything. Such encryption would mean  
27 that only the parties in a conversation could see what was being said, with even Yahoo  
28 unable to read it.

Mr. Bonforte said he resisted the request because it would have hurt Yahoo’s ability to  
index and search message data to provide new user services. “I’m not particularly  
thrilled with building an apartment building which has the biggest bars on every  
window,” he said.

The 2014 hiring of Mr. Stamos — who had a reputation for pushing for privacy and  
antisurveillance measures — was widely hailed by the security community as a sign that  
Yahoo was prioritizing its users’ privacy and security.

The current and former employees say he inspired a small team of young engineers to  
develop more secure code, improve the company’s defenses — including encrypting  
traffic between Yahoo’s data centers — hunt down criminal activity and successfully  
collaborate with other companies in sharing threat data.

\* \* \*

1 *But when it came time to commit meaningful dollars to improve Yahoo's security*  
 2 *infrastructure, Ms. Mayer repeatedly clashed with Mr. Stamos, according to the*  
 3 *current and former employees. She denied Yahoo's security team financial resources*  
 4 *and put off proactive security defenses, including intrusion-detection mechanisms for*  
 5 *Yahoo's production systems. Over the last few years, employees say, the Paranoids*  
 6 *have been routinely hired away by competitors like Apple, Facebook and Google.*

7 Mr. Stamos, who departed Yahoo for Facebook last year, declined to comment. But  
 8 during his tenure, *Ms. Mayer also rejected the most basic security measure of all: an*  
 9 *automatic reset of all user passwords, a step security experts consider standard after a*  
 10 *breach. Employees say the move was rejected by Ms. Mayer's team for fear that even*  
 11 *something as simple as a password change would drive Yahoo's shrinking email users*  
 12 *to other services.*<sup>38</sup>

13 77. Defendants' failure to respond appropriately (e.g., by failing to implement automatic  
 14 password resets) and their resistance to adopting needed security measures exposed investors to the  
 15 possibility of a significant depletion in the value of Yahoo's core business, causing additional harm to  
 16 investors.

17 78. As a result of the Defendants' refusal to implement appropriate data security safeguards,  
 18 several prominent Yahoo security experts left the Company during the Class Period. For example,  
 19 Yahoo's Chief Information Security Officer Alex Stamos left Yahoo for Facebook after repeatedly  
 20 clashing with Defendant Mayer over security issues. Stamos was hired in 2014 by Yahoo to address  
 21 security failures, including Yahoo's vulnerabilities to repeated hacks by Russian hackers.<sup>39</sup>

22 79. Equally troubling, according to a former Yahoo executive quoted in a September 30,  
 23 2016 Business Insider article, *Yahoo kept all user data in one database*, increasing the devastating  
 24 impact of a data breach. According to this executive, "the architecture of Yahoo's back-end systems is  
 25 organized in such a way that the type of breach that was reported would have exposed a much larger  
 26 group of user account information." The article also highlighted the executive's skepticism that the  
 27 2013 Data Breach impacted "only" 500 million users:

28 <sup>38</sup> See <http://www.nytimes.com/2016/09/29/technology/yahoo-data-breach-hacking.html>.

<sup>39</sup> *Yahoo seen cutting cost corners with security tech discredited long before massive attack*, Reuters, Dec. 19, 2016.

1 “I believe it to be bigger than what’s being reported,” the executive, who no longer  
2 works for the company but claims to be in frequent contact with employees still there,  
3 including those investigating the breach, told Business Insider. “How they came up  
4 with 500 is a mystery.”

5 To be sure, Yahoo has said that the breach affected at least 500 million users. But the  
6 former Yahoo exec estimated the number of accounts that could have potentially been  
7 stolen could be anywhere between 1 billion and 3 billion.

8 \*\*\*

9 According to this executive, all of Yahoo’s products use one main user database, or  
10 UDB, to authenticate users. So people who log into products such as Yahoo Mail,  
11 Finance, or Sports all enter their usernames and passwords, which then goes to this one  
12 central place to ensure they are legitimate, allowing them access.

13 That database is huge, the executive said. At the time of the hack in 2014, inside were  
14 credentials for roughly 700 million to 1 billion active users accessing Yahoo products  
15 every month, along with many other inactive accounts that hadn’t been deleted.

16 In late 2013, Yahoo CEO Marissa Mayer said the company had 800 million monthly  
17 active users globally. It currently has more than 1 billion.

18 “*That is what got compromised,*” the executive said. “*The core crown jewels of Yahoo*  
19 *customer credentials.*”

20 Yahoo’s UDB is still the main repository for user credentials and is still in use, LinkedIn  
21 profiles from current Yahoo employees and a 2015 court ruling show.<sup>40</sup>

22 80. As investors ultimately learned, the executive was right: Defendants’ security breaches  
23 impacted more than one billion Yahoo customers.

### 24 **The 2013 Data Breach**

25 81. Despite well-publicized litigation and frequent public announcements of data breaches  
26 by retailers and technology companies, and the Company’s own exposure to repeated hacks, Yahoo  
27 opted to maintain an insufficient and inadequate system to protect its users’ Private Information.

28 82. As a result, in August 2013, hackers breached the email system of Yahoo, *stealing the*  
records of more than one billion users, including names, birth dates, phone numbers, and passwords  
that were encrypted with the easily broken MD5 security (“2013 Data Breach”). The hackers also  
obtained the security questions and backup email addresses used to reset lost passwords. The attackers

<sup>40</sup> Paul Szoldra, *A Yahoo insider believes the hackers could really have stolen over 1 billion accounts*,  
Business Insider (Sept. 30, 2016), <http://www.businessinsider.com/yahooinsider-hacking-2016-9>.

1 forged the cookies that Yahoo places on user computers, including the authentication cookies. By  
2 forging the authentication cookies, the hackers could gain access to the targeted accounts without ever  
3 having the user's password and would also allow the hacker to remain logged into a user's account  
4 indefinitely.

5 83. Defendants knew about the 2013 Data Breach but failed to disclose it until confronted by  
6 law enforcement. In August 2016, Andrew Komarov, a chief intelligence officer at InfoArmor,  
7 independently discovered the breach. InfoArmor is an Arizona cybersecurity firm that delivers identity,  
8 financial, and privacy protection, as well as threat intelligence and investigative services to help  
9 businesses fight evolving online threats. As the chief intelligence officer for InfoArmor, Komarov's  
10 job is to prowl the internet's darkest corners, infiltrate cybercrime rings, and help law enforcement and  
11 InfoArmor's clients track down stolen data.  
12

13  
14 84. Komarov had been monitoring an Eastern European hacker group when he saw them  
15 offering up a huge database for sale: the Yahoo user accounts. The group Komarov had been  
16 surveilling, which he calls Group E, was keeping the sale off of public cybercrime forums.

17 85. Group E claimed to have possession of a database of logins for up to one billion Yahoo  
18 accounts for sale for \$300,000. Komarov watched Group E sell the database three times, and he was  
19 able to intercept the database during the sales. Two buyers were large spamming groups that are on the  
20 list for Spamhaus Register of Known Spam Operations, or ROKSO. The other buyer had an unusual  
21 request before completing the purchase. This third buyer gave the sellers a list of ten names of U.S. and  
22 foreign government officials and business executives, to verify their logins were part of the database.  
23 That led Komarov to speculate the buyer was a foreign intelligence agency.  
24

25  
26 86. Having intercepted the potential sale of the Yahoo database, InfoArmor approached  
27 Yahoo through an intermediary to work together, investigate and resolve the massive theft. According  
28 to Komarov, instead of leaping into action, *Yahoo was utterly dismissive* of the intermediary. At the

1 time, Yahoo was not interested in investigating the breach because it was finalizing a sale of its core  
2 business to Verizon in a multi-billion dollar transaction. Yahoo did not want to jeopardize the deal by  
3 disclosing the massive breach. Its intermediary having been rejected by Yahoo, InfoArmor notified  
4 military and law enforcement authorities in the United States, Australia, Canada, Britain and the  
5 European Union about the breach. After those parties verified the authenticity of the stolen records,  
6 some of them went to Yahoo directly with their concerns.

7  
8 87. On December 14, 2016, months after rebuking InfoArmor's alert and only after federal  
9 authorities confronted Yahoo about the breach, the Company finally announced that it had been hacked:

10 Yahoo! Inc. has identified data security issues concerning certain Yahoo user accounts.  
11 Yahoo has taken steps to secure user accounts and is working closely with law  
12 enforcement.

13 As Yahoo previously disclosed in November, law enforcement provided the company  
14 with data files that a third party claimed was Yahoo user data. The company analyzed  
15 this data with the assistance of outside forensic experts and found that it appears to be  
16 Yahoo user data. Based on further analysis of this data by the forensic experts, ***Yahoo  
believes an unauthorized third party, in August 2013, stole data associated with more  
than one billion user accounts.*** The company has not been able to identify the intrusion  
17 associated with this theft. Yahoo believes this incident is likely distinct from the incident  
18 the company disclosed on September 22, 2016.

19 For potentially affected accounts, the stolen user account information may have included  
20 names, email addresses, telephone numbers, dates of birth, hashed passwords (using  
21 MD5) and, in some cases, encrypted or unencrypted security questions and answers. The  
22 investigation indicates that the stolen information did not include passwords in clear text,  
23 payment card data, or bank account information. Payment card data and bank account  
24 information are not stored in the system the company believes was affected.

25 ***Yahoo is notifying potentially affected users and has taken steps to secure their  
accounts, including requiring users to change their passwords.*** Yahoo has also  
26 invalidated unencrypted security questions and answers so that they cannot be used to  
27 access an account.

28 \* \* \*

29 Yahoo encourages users to review all of their online accounts for suspicious activity and  
30 to change their passwords and security questions and answers for any other accounts on  
which they use the same or similar information used for their Yahoo account. The  
company further recommends that users avoid clicking links or downloading  
attachments from suspicious emails and that they be cautious of unsolicited  
communications that ask for personal information. Additionally, Yahoo recommends



1 using Yahoo Account Key, a simple authentication tool that eliminates the need to use a  
2 password on Yahoo altogether.

3 88. Commenting on the 2013 Data Breach, InfoArmor’s Andrew Komarov said the Yahoo  
4 hack is different than other hacks: “The Yahoo hack makes cyber espionage extremely efficient . . .  
5 Personal information and contacts, e-mail messages, objects of interest, calendars and travel plans are  
6 key elements for intelligence-gathering in the right hands. The difference of the Yahoo hack between  
7 any other hack is in that it may really destroy your privacy, and potentially have already destroyed it  
8 several years ago without your knowledge.”<sup>41</sup>

9 89. Many articles discussing the breach were published on the heels of the Company’s  
10 public disclosure. The New York Times published an article titled “Yahoo Says 1 Billion User  
11 Accounts Were Hacked,” which discussed how the disclosure of the 2013 Data Breach revealed  
12 Yahoo’s lax security measures:  
13

14 *Security has taken a back seat at Yahoo in recent years, compared to Silicon Valley*  
15 *competitors like Google and Facebook. Yahoo’s security team clashed with top*  
16 *executives, including the chief executive, Marissa Mayer, over the cost and customer*  
17 *inconvenience of proposed security measures.*

18 And critics say the company was slow to adopt aggressive security measures, even after  
19 a breach of over 450,000 accounts in 2012 and series of spam attacks — a mass mailing  
20 of unwanted messages — the following year.

21 “What’s most troubling is that this occurred so long ago, in August 2013, and no one  
22 saw any indication of a breach occurring until law enforcement came forward,” said Jay  
23 Kaplan, the chief executive of Synack, a security company. “Yahoo has a long way to go  
24 to catch up to these threats.”<sup>42</sup>

25 90. The article also revealed that, in response to the discovery of the 2013 Data Breach,  
26 Yahoo is requiring “all of the affected users to change their passwords and it is invalidating  
27  
28

<sup>41</sup> See <http://www.bloomberg.com/news/articles/2016-12-15/stolen-yahoo-data-includes-government-employee-information>.

<sup>42</sup> Vindu Goel and Nicole Perlroth, *Yahoo Says 1 Billion User Accounts Were Hacked*, N.Y. Times (Dec. 14, 2016), <http://www.nytimes.com/2016/12/14/technology/yahoo-hack.html>.

1 unencrypted security questions — steps that it declined to take in September,” when it announced the  
2 2014 Data Breach.<sup>43</sup>

3 91. An article published on Time, Inc.’s Money magazine website further discussed the  
4 severity of the attack:

5 ***Most alarming of all, the breaches may have put information related to national***  
6 ***security at risk.*** Bloomberg reported that upward of 150,000 U.S. government and  
7 military employees — including members of the FBI, CIA, White House, and others  
8 working with extremely sensitive information — are among those affected by the Yahoo  
9 hack, because they gave Yahoo their work email addresses as backups in case they were  
ever locked out of their Yahoo accounts. Now that information is in the hands of  
cybercriminals.

10 It’s a leak that could allow foreign intelligence services to identify employees and hack  
11 their personal and work accounts, posing a threat to national security.

12 92. Analysts dubbed the 2013 Data Breach “***the Exxon Valdez of security breaches,***” given  
13 the fact that “1 billion accounts [were] compromised, when there are only 3 billion people with Internet  
14 access in the world.”<sup>44</sup>

### 15 **The 2014 Data Breach**

16 93. In late 2014, a “state-sponsored actor” ***stole the account information of 500 million***  
17 ***Yahoo users,*** including names, e-mail addresses, telephone numbers, dates of birth, passwords (created  
18 with MD5 algorithms), and security questions and answers (“2014 Data Breach”). Cybersecurity  
19 experts likened the 2014 data breach to an “***ecological disaster.***”  
20

21 94. Details of the 2014 Data Breach are set forth in a March 2017 Indictment by the U.S.  
22 Justice Department (the “Indictment”). The Indictment charges two Russian intelligence agents and  
23 two hackers with masterminding the 2014 theft of 500 million Yahoo accounts, marking the first time  
24 the U.S. government criminally charged Russian spies for cyber offenses. The 47-count Indictment  
25

26  
27 <sup>43</sup> *Id.*

28 <sup>44</sup> James Rogers, *Yahoo hack: The ‘Exxon Valdez of security breaches,’* Fox News (Dec. 15, 2016),  
<http://www.foxnews.com/tech/2016/12/15/yahoo-hack-exxon-valdez-security-breaches.html>.

1 includes charges of conspiracy, computer fraud and abuse, economic espionage, theft of trade secrets,  
2 wire fraud, access device fraud and aggravated identity theft.

3 95. According to the Indictment, from at least in or about January 2014 up to and including  
4 at least in or about December 2016, officers of the Russian Federal Security Service (“FSB”), an  
5 intelligence and law enforcement agency of the Russian Federation (“Russia”) headquartered in  
6 Lubyanka Square, Moscow, Russia, and a successor service to the Soviet Union's Committee of State  
7 Security (“KGB”), conspired together and with each other to protect, direct, facilitate, and pay criminal  
8 hackers to collect information through computer intrusions in the United States and elsewhere. The  
9 FSB officers, defendants Dmitry Dokuchaev, Igor Sushchin, and others known and unknown to the  
10 Grand Jury, directed the criminal hackers, defendants Alexsey Belan, Karim Baratov, and others known  
11 and unknown to the Grand Jury (collectively, the “conspirators”), to gain unauthorized access to the  
12 computers of companies providing webmail and internet-related services located in the Northern  
13 District of California and elsewhere, to maintain unauthorized access to those computers, and to steal  
14 information from those computers, including information regarding, and communications of, the  
15 providers' users.  
16

17  
18 96. The Indictment states that in or around early 2014, the conspirators gained unauthorized  
19 access to Yahoo's network and began their reconnaissance. After gaining unauthorized access to  
20 Yahoo's network, Belan located and stole relevant Yahoo network resources of interest, including  
21 Yahoo's user database and its account management tools. Information stolen in the breach included  
22 names, email addresses, phone numbers, birth dates, encrypted password, and security questions and  
23 answers. The conspirators used their unauthorized access to Yahoo's network to identify and access  
24 accounts of, among other victims, users affiliated with U.S. online service providers, including but not  
25 limited to webmail providers and cloud computing companies, whose account contents could facilitate  
26 unauthorized access to other victim accounts; Russian journalists and politicians critical of the Russian  
27  
28

1 government; Russian citizens and government officials; former officials from countries bordering  
2 Russia; and U.S. government officials, including cyber security, diplomatic, military, and White House  
3 personnel.

4 97. In addition to executing the FSB's directives, Belan leveraged his access to Yahoo's  
5 network to enrich himself: (a) through an online marketing scheme, by manipulating Yahoo search  
6 results for erectile dysfunction drugs; (b) by searching Yahoo user email accounts for credit card and  
7 gift card account numbers and other information that could be monetized; and (c) by gaining  
8 unauthorized access to the accounts of more than 30 million Yahoo users, the contacts of whom were  
9 then stolen as part of a spam marketing scheme.

10  
11 98. At the time of the 2014 Data Breach, Belan was one of FBI's Cyber Most Wanted  
12 criminals since 2012. An Interpol Red Notice seeking his immediate detention had been lodged  
13 (including with Russia) since July 26, 2013. The FBI accused Belan of hacking into three major e-  
14 commerce companies between 2012 and 2013, stealing the user data and the encrypted passwords of  
15 millions of accounts and selling the information. Two separate federal arrest warrants and indictments  
16 for Belan have been issued in connection with those thefts. One was issued on September 12, 2012, in  
17 the U.S. District Court, District of Nevada, Las Vegas, after Belan was charged with obtaining  
18 information by computer from a protected computer; possession of fifteen or more unauthorized access  
19 devices; and aggravated identity theft. The second warrant was issued on June 6, 2013, in the U.S.  
20 District Court, Northern District of California, San Francisco, after Belan was charged with two counts  
21 of fraud in connection with a computer and two counts of aggravated identity theft.<sup>45</sup>

22  
23  
24 99. Karim Baratov, one of the alleged hackers located in Canada, was recently arrested. The  
25 U.S. Department of Justice ("DOJ") has issued arrest warrants for Dokuchaev, Sushchin and Belan in  
26 connection with the 2014 Data Breach.  
27

28 <sup>45</sup> See <http://www.fbi.gov/wanted/cyber/alexsey-belan>.

1 100. Yahoo knew about the 2014 Data Breach at the time it occurred and even assigned it an  
2 internal code name, the “Siberian Intrusion.” Despite having contemporaneous knowledge of the  
3 breach, Yahoo kept its customers and investors in the dark about it *for years*, refusing to disclose the  
4 hack until rumors emerged in the market.

5 101. In July 2016, account names and passwords for about 200 million Yahoo user accounts  
6 were presented for sale on the dark-net market site, “TheRealDeal.” The seller, known as “Peace of  
7 Mind” or simply “Peace,” stated in a confidential interview with Wired Magazine that he had possessed  
8 the stolen database for an extended period of time and had been selling it privately since about late  
9 2015. Peace had previously been connected to sales of similar private information data from other  
10 hacks, including that from the 2012 LinkedIn hack.

11 102. Joseph Cox, a reporter with the technology news site Motherboard, said he emailed  
12 Yahoo on July 30, 2016, to ask if the Company was aware that Peace was attempting to sell Yahoo  
13 data. In a response email to Motherboard, a Yahoo spokesperson said “*We are aware of a claim . . .*  
14 *We are committed to protecting the security of our users’ information and we take any such claim very*  
15 *seriously. Our security team is working to determine the facts. Yahoo works hard to keep our users*  
16 *safe, and we always encourage our users to create strong passwords, or give up passwords altogether by*  
17 *using Yahoo Account Key, and use different passwords for different platforms.” Yahoo provided no*  
18 *other details and declined to say if the claim exposing a breach was legitimate.*<sup>46</sup>

19 103. According to reports, Yahoo's awareness of "Peace's" claim extended to the Company's  
20 CEO, defendant Mayer.<sup>47</sup>

21  
22  
23  
24  
25  
26 <sup>46</sup> Joseph Cox, *Yahoo “Aware” Hacker is Advertising 200 Million Supposed Accounts on Dark Web*,  
27 Motherboard, Aug. 1, 2016.

28 <sup>47</sup> Madhumita Murgiz, et al., *Marissa Mayer Knew of Yahoo Breach Probe in July*, Financial Times  
(Sept. 23, 2016), <http://www.ft.com/content/d0d07444-81aa-11e6-bc52-0c7211ef3198>.

1 104. Peace told Motherboard, "well f\*\*\* them they dont want to confirm well better for me  
2 they dont do password reset."<sup>48</sup>

3 105. Nearly two months later, on September 22, 2016—and only after Yahoo finalized the  
4 sale of its business to Verizon—the Company confirmed that data associated with 500 million users'  
5 accounts was stolen. Only at that time, Yahoo told users to change their password and security  
6 questions and review their accounts for suspicious activity:  
7

8 A recent investigation by Yahoo! Inc. has confirmed that a copy of certain user account  
9 information was stolen from the company's network in late 2014 by what it believes is a  
10 state-sponsored actor. The account information may have included names, email  
11 addresses, telephone numbers, dates of birth, hashed passwords (the vast majority with  
12 bcrypt) and, in some cases, encrypted or unencrypted security questions and answers.  
13 The ongoing investigation suggests that stolen information did not include unprotected  
14 passwords, payment card data, or bank account information; payment card data and bank  
15 account information are not stored in the system that the investigation has found to be  
16 affected. Based on the ongoing investigation, Yahoo believes that information associated  
17 with at least 500 million user accounts was stolen and the investigation has found no  
18 evidence that the state-sponsored actor is currently in Yahoo's network. Yahoo is  
19 working closely with law enforcement on this matter.

20 Yahoo is notifying potentially affected users and has taken steps to secure their accounts.  
21 These steps include invalidating unencrypted security questions and answers so that they  
22 cannot be used to access an account and asking potentially affected users to change their  
23 passwords. Yahoo is also recommending that users who haven't changed their  
24 passwords since 2014 do so.

25 Yahoo encourages users to review their online accounts for suspicious activity and to  
26 change their password and security questions and answers for any other accounts on  
27 which they use the same or similar information used for their Yahoo account. The  
28 company further recommends that users avoid clicking on links or downloading  
attachments from suspicious emails and that they be cautious of unsolicited  
communications that ask for personal information. Additionally, Yahoo asks users to  
consider using Yahoo Account Key, a simple authentication tool that eliminates the need  
to use a password altogether.

Online intrusions and thefts by state-sponsored actors have become increasingly  
common across the technology industry. Yahoo and other companies have launched  
programs to detect and notify users when a company strongly suspects that a state-  
sponsored actor has targeted an account. Since the inception of Yahoo's program in  
December 2015, independent of the recent investigation, approximately 10,000 users  
have received such a notice.

---

<sup>48</sup> Joseph Cox, *Yahoo "Aware" Hacker is Advertising 200 Million Supposed Accounts on Dark Web*, Motherboard, Aug. 1, 2016.

1 106. Verizon stated that Yahoo told it about the breach just two days earlier, on September  
2 20, 2016.

3 107. Yahoo was lambasted for taking at least two months to report the breach to the public.  
4 Senator Richard Blumenthal stated that “[i]f Yahoo knew about the hack as early as August [2016],  
5 and failed to coordinate with law enforcement, taking this long to confirm the breach is a blatant  
6 betrayal of their users’ trust.”<sup>49</sup> Senator Blumenthal called on law enforcement and regulators to  
7 “investigate whether Yahoo may have concealed its knowledge of this breach in order to artificially  
8 bolster its valuation in its pending acquisition by Verizon.”  
9

10 108. While Senator Blumenthal’s anger over a two month delay was justified, it is now clear  
11 that the Company had actually known about the 2014 Data Breach when it occurred. Indeed, as  
12 explained in more detail below, Yahoo eventually revealed on November 9, 2016 that *it identified in*  
13 *late 2014* that a state sponsored actor had hacked into Yahoo’s network.  
14

15 109. The 2014 Data Breach shares similarities to the 2013 hack. Indeed, in a February 23,  
16 2017 letter to John Thune, Senate Chairman of the Committee on Commerce, Science and  
17 Transportation and Jerry Moran, Senate Chairman of the Subcommittee on Consumer Protection,  
18 Product Safety, Insurance and Data Security, Yahoo stated that “[a] majority of the user accounts that  
19 were potentially affected by the 2014 Incident are also believed to have been affected by the 2013  
20 Incident.”<sup>50</sup>  
21

### 22 **The Forged Cookie Data Breach**

23 110. On March 1, 2017, the Company began notifying approximately 32 million Yahoo users  
24 that they had been the victim of yet another breach, this time a “forged cookie” data breach in 2015-  
25

26 <sup>49</sup> Seth Fiegerman, *Yahoo Says 500 Million Accounts Stolen*, CNN Tech (Sept. 23, 2016),  
27 <http://money.cnn.com/2016/09/22/technology/yahoo-data-breach>.

28 <sup>50</sup> Letter from Yahoo! Inc. to U.S. Sens. John Thune & Jerry Moran (Feb 23, 2017), available at  
[https://www.commerce.senate.gov/public/cache/files/ed55102d-33ae-406e-a700-  
b194cd6afcfc/680BEF0769C55302BBA040C0BCE9E9D8.yahoo-letter.pdf](https://www.commerce.senate.gov/public/cache/files/ed55102d-33ae-406e-a700-b194cd6afcfc/680BEF0769C55302BBA040C0BCE9E9D8.yahoo-letter.pdf).

1 2016 (the “Forged Cookie Breach”). “Based on the investigation, we believe an unauthorised third  
2 party accessed the company's proprietary code to learn how to forge certain cookies,” the Company  
3 said. “Forged cookies could allow an intruder to access users’ accounts without a password,” Yahoo  
4 explained. The Company has connected some of this activity to the same state-sponsored actor  
5 believed to be responsible for the 2014 Data Breach.

6  
7 111. Some Yahoo users posted comments on Twitter about the warning messages they  
8 received from Yahoo about the Forged Cookie Breach. “Within six people in our lab group, at least  
9 one other person has gotten this email,” Joshua Plotkin, a biology professor at the University of  
10 Pennsylvania, said. “That’s just anecdotal of course, but for two people in a group of six to have gotten  
11 it, I imagine it’s a considerable amount.”

12  
13 112. Yahoo said that it has forced password resets and invalidated the forged cookies.

#### 14 **Defendants Had Contemporaneous Knowledge of the Breaches**

15 113. Defendants failed to notify investors about the 2013 Data Breach, the 2014 Data Breach,  
16 and the Forged Cookie Data Breach for years, despite their contemporaneous knowledge of the hacks.

17 114. In Yahoo’s quarterly results for the third quarter of 2016 filed with the SEC on  
18 November 9, 2016, Defendants finally disclosed that they *had contemporaneous knowledge of the*  
19 *2014 Data Breach:*

20  
21 In late July 2016, a hacker claimed to have obtained certain Yahoo user data. After  
22 investigating this claim with the assistance of an outside forensic expert, the Company  
23 could not substantiate the hacker’s claim. Following this investigation, the Company  
24 intensified an ongoing broader review of the Company’s network and data security,  
25 including a review of *prior access to the Company’s network by a state-sponsored actor*  
26 *that the Company had identified in late 2014*. Based on further investigation with an  
27 outside forensic expert, *the Company disclosed the Security Incident on September 22,*  
28 *2016, and began notifying potentially affected users, regulators, and other*  
*stakeholders.*

The Company, with the assistance of outside forensic experts, continues to investigate  
the Security Incident and related matters. The Company is actively working with U.S.  
law enforcement authorities on this matter.



1 As described above, the Company had identified that a state-sponsored actor had access  
 2 to the Company's network in late 2014. An Independent Committee of the Board,  
 3 advised by independent counsel and a forensic expert, is investigating, among other  
 4 things, the scope of knowledge within the Company in 2014 and thereafter regarding this  
 5 access, the Security Incident, the extent to which certain users' account information had  
 6 been accessed, the Company's security measures, and related incidents and issues.

7 In addition, the forensic experts are currently investigating certain evidence and activity  
 8 that indicates an intruder, believed to be the same state-sponsored actor responsible for  
 9 the Security Incident, created cookies that could have enabled such intruder to bypass  
 10 the need for a password to access certain users' accounts or account information.

11 115. Then, on March 1, 2017, Yahoo provided additional details regarding Defendants'  
 12 contemporaneous knowledge of the breaches, admitting that they had contemporaneous knowledge not  
 13 only of the 2014 Data Breach but also of the Forged Cookie Data Breach:

14 As previously disclosed, an independent committee (the "Independent Committee") of  
 15 the Board of Directors (the "Board") has investigated the Security Incidents<sup>51</sup> and related  
 16 matters, including the scope of knowledge within the Company in 2014 of access to  
 17 Yahoo's network by the state-sponsored actor responsible for the theft and related  
 18 incidents, the Company's internal and external reporting processes and remediation  
 19 efforts related to the 2014 Security Incident and related incidents. The Independent  
 20 Committee has concluded its investigation, although it will continue to review  
 21 developments regarding the Security Incidents and report to the Board on these issues,  
 22 and cooperate with various government entities . . . .

23 Based on its investigation, the Independent Committee concluded that *the Company's*  
 24 *information security team had contemporaneous knowledge of the 2014 compromise*  
 25 *of user accounts, as well as incidents by the same attacker involving cookie forging in*  
 26 *2015 and 2016. In late 2014, senior executives and relevant legal staff were aware that*  
 27 *a state-sponsored actor had accessed certain user accounts by exploiting the*  
 28 *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 . . .

\* \* \*

*Actions the Company is Taking in Response to the Independent Committee's Findings*

<sup>51</sup> The Security Incidents consist of the 2013 Data Breach, the 2014 Data Breach, and the Forged  
 Cookie Data Breach.

1 Based on the Independent Committee’s findings, the Board has taken the management  
2 related actions described below, adopted certain process and structure changes to address  
3 the Company’s issues with respect to the Security Incidents, and taken certain other  
4 disciplinary actions.

5 *Management Changes*

6 In response to the Independent Committee’s findings related to the 2014 Security  
7 Incident, the Board determined not to award to the Chief Executive Officer a cash bonus  
8 for 2016 that was otherwise expected to be paid to her. In addition, in discussions with  
9 the Board, the Chief Executive Officer offered to forgo any 2017 annual equity award  
10 given that the 2014 Security Incident occurred during her tenure and the Board accepted  
11 her offer.

12 On March 1, 2017, Ronald S. Bell resigned as the Company’s General Counsel and  
13 Secretary and from all other positions with the Company. No payments are being made  
14 to Mr. Bell in connection with his resignation.

15 *Other Remedial Actions*

16 Additionally, in response to the Independent Committee’s findings and  
17 recommendations, the Board has directed the Company to implement or enhance a  
18 number of corrective actions, including revision of its technical and legal information  
19 security incident response protocols to help ensure: escalation of cybersecurity incidents  
20 to senior executives and the Board of Directors; rigorous investigation of cybersecurity  
21 incidents and engagement of forensic experts as appropriate; rigorous assessment of and  
22 documenting any legal reporting obligations and engagement of outside counsel as  
23 appropriate; comprehensive risk assessments with respect to cybersecurity events;  
24 effective cross-functional communication regarding cybersecurity events; appropriate  
25 and timely disclosure of material cybersecurity incidents; and enhanced training and  
26 oversight to help ensure processes are followed.

27 116. FBI Officer John Bennett, the Special Agent in charge of the San Francisco’s FBI  
28 division involved heavily in the investigation of the 2014 Data Breach, specifically called out  
29 Defendant Mayer for her *ongoing involvement* in the investigation, saying she demonstrated  
30 “leadership and courage while under pressure from many entities.” Bennett’s statements, made at a  
31 March 15, 2017 press conference in San Francisco, leave no room for doubt that Mayer was aware of  
32 the 2014 Data Breach—and its severity—from the very beginning:

33 Early this week I spoke with Marissa Mayer and expressed my appreciation for Yahoo’s  
34 cooperation in this matter. This was not our first conversation. Ms. Mayer has  
35 demonstrated great leadership and courage while under intense pressure from many  
36 entities. *She and her team at Yahoo have always been professional, engaged and  
37 responsive to our requests. They were great partners to be with during this two year  
38 investigation.* This case illustrates that the FBI can work with victims, including those

1 right here in Silicon Valley to address malicious cyber activities while respecting  
2 victim’s sensitivities.

3 117. Officer Bennett said the government did not ask Yahoo to keep the breach secret from  
4 the public.

5 118. FBI agent Elvis Chan, a member of the investigation team in San Francisco, which  
6 focuses on Eurasian hacking, said the FBI noticed some telltale evidence of Russian hackers as soon as  
7 they started the investigation. That evidence included the IP addresses near Moscow as well as other  
8 indications that the hack was from Russia.

9 119. Reportedly, the British intelligence agency MI5 was brought in to help the U.S. probe as  
10 the actions of Russia’s intelligence agency were classified as “hostile actors.”

11 120. The hackers maintained their access to Yahoo’s networks until at least October 2016, the  
12 FBI said.

13 121. Other evidence confirms Defendants’ contemporaneous knowledge of the breaches.  
14 According to a verified derivative complaint filed against Yahoo after counsel for the plaintiff in that  
15 action reviewed documents produced by Yahoo in response to a demand for corporate books and  
16 records, Yahoo’s Board of Directors, including Defendant Mayer, *received consistent security updates*  
17 *from the Company’s Chief Information Security Officers* (“CISO”).<sup>52</sup> For example, the Board of  
18 Directors received CISO or other cybersecurity updates during at least six meetings, including those  
19 held on April 8, 2014, June 25, 2014, October 16, 2014, June 23, 2015, October 14-15, 2015, and April  
20 13-14, 2016.<sup>53</sup> The Board of Directors had knowledge of and received repeated updates regarding “the  
21 [REDACTED] Intrusion” starting at least in October 2014 and continuing until at least April 2016.<sup>54</sup>  
22  
23  
24  
25

26 <sup>52</sup> *Oklahoma Firefighters Pension and Retirement System, derivatively on behalf of Yahoo! Inc., v.*  
27 *Brandt, et al.*, No. 2017-cv-0133-SG (Feb. 23, 2017).

28 <sup>53</sup> *Id.* at ¶48.

<sup>54</sup> *Id.* at ¶127.

1 122. Confidential witnesses with relevant knowledge also attest that Defendants knew about  
2 the 2013 and 2014 breaches from the start. These witnesses include CW1, who served as an Executive  
3 Assistant at Yahoo from May 2010 to August 2014 in the Company's Sunnyvale, California  
4 headquarters, reporting to the Senior Vice President of Customer Experience. CW1 stated that Yahoo  
5 was trying to trouble shoot the hacked email accounts during both the 2013 and 2014 breaches. "We  
6 discovered [a breach], then you notified [supervisors] and started to take action on getting [the breach]  
7 taken care of," CW1 said. According to CW1, Defendant Mayer was "made aware" of attempts to fix  
8 the breaches on a daily basis. "Sometimes it was my executive that informed [Mayer]," CW1 said.  
9 "Typically, it would have been through email, or they'd have these daily check in meetings to see how  
10 things were going along." Those meetings were typically attended by CW1's executive boss, the Chief  
11 Marketing Officer Kathy Savitt, and Defendant Mayer. Sometimes another executive or two might  
12 attend, but mostly the meetings were "just the folks close to what was happening."  
13  
14

15 123. "I was with the company for four years, from 2010 to 2014, and there were two [major  
16 breaches] during that time," CW1 said. "The organization which I was in, customer experience, dealt  
17 with both." When breaches occurred, it got very hectic very quickly in customer experience. "When  
18 these situations happened, we had to go into damage control and pull out a lot of resources to get this  
19 taken care of," CW1 continued. "When it's out there, that these accounts are getting hacked, we just  
20 want to get it taken care of." "It was a pretty high priority." According to CW1, Mayer wanted to stay  
21 in the loop on the team's progress. "*She wanted updates once she was informed, and that was in*  
22 *addition to the daily meetings or daily updates.*"  
23

24 124. When asked if Mayer downplayed the significance of the breaches, CW1 said, "*she*  
25 *definitely didn't want to publicize it.*"  
26

27 125. Despite the belated acknowledgment that "[i]n late 2014 senior executives and relevant  
28 legal staff were aware that a state-sponsored actor had accessed certain user accounts by exploiting the

1 Company’ account management tool,” Yahoo has self-servingly focused blame on the “relevant legal  
2 team,” specifically Defendant Bell, Yahoo’s General Counsel. Yahoo asserts that at the time the  
3 breaches were occurring, Yahoo’s legal team “had sufficient information to warrant substantial further  
4 inquiry in 2014, and they did not sufficiently pursue it.” In addition, Yahoo disclosed that Bell  
5 “resigned” from his position and that “no payments are being made to Mr. Bell in connection with his  
6 resignation.”

7  
8 126. Yahoo’s own former executives reacted with disbelief at placing blame solely on Bell.  
9 Yahoo’s former head of media, Scott Moore, called the condemnation “*ridiculous*,” saying “I know  
10 @ronsbell\_tech who is a good man and *as a lawyer he wasn’t in charge of security* @Yahoo @lame  
11 CYA move @marrisamayer twitter.com/karaswisher/st...”

12  
13 127. Reportedly, “most people inside Yahoo think Mayer and the board should have  
14 shouldered the bulk of the blame for the breach.” Instead, Defendant Mayer would pocket an  
15 astounding \$186 million in compensation during the Class Period. She was one of the five highest-  
16 paid women in 2016. Former Yahoo president Sue Decker called Mayer’s \$186 million payout  
17 “egregious,” “given what happened in the performance of the company.” While in possession of  
18 material, non-public information regarding inadequacies in the Company’s information security  
19 protocols, which compromised the Private Information of Yahoo’s users,’ during the Class Period  
20 Mayer sold at least 1.2 million shares of Yahoo common stock at artificially inflated prices, for  
21 proceeds of more than \$51 million. Mayer’s sales were timed to maximize profits from the Company’s  
22 then artificially inflated stock price. Mayer stands to receive \$23 million in golden-parachute  
23 compensation from the Verizon deal.  
24

25  
26 128. Even more troubling—and emblematic of Yahoo’s continued intent to deceive—is its  
27 false representation in a September 9, 2016 regulatory filing with the SEC that “there have not been any  
28 incidents of, or third-party claims alleging, (i) Security Breaches, unauthorized access or unauthorized

1 use of any of Seller's or the Business Subsidiaries' information technology systems or (ii) loss, theft,  
2 unauthorized access or acquisition, modification, disclosure, corruption, or other misuse of any  
3 Personal Data" in Yahoo's possession.

4 129. In October 2016, Verizon's general counsel and executive VP of public policy, Craig  
5 Silliman, told reporters that "I think we have a reasonable basis to believe right now that the impact [of  
6 the 2014 breach] is material . . . ."

8 130. Yahoo saw its shares plunge immediately after each breach disclosure.

### 9 **Yahoo Is Assailed for Failure to Fulfill Its Disclosure Obligations**

10 131. On September 23, 2016, the Los Angeles Times published an article titled "It's strange  
11 Yahoo took 2 years to discover a data breach, security experts say." According to internet security  
12 experts interviewed for the article, it takes an average of 201 days to detect a data breach, and this  
13 period is usually shorter for technology-focused companies such as Yahoo.

14 132. According to the Ponemon Institute, which tracks data breaches, the average time it  
15 takes organizations to identify a data breach is 191 days after the date of the breach, and the average  
16 time to contain a breach is 58 days after its discovery.<sup>55</sup>

17 133. As a result of Yahoo's failure to disclose the breaches for several years, its users  
18 continued using their accounts unaware that hackers had access to their Private Information.  
19

20 134. Yahoo's improprieties were quick to attract the ire of U.S. senators. Senator Mark  
21 Warner of Virginia was quoted stating that "[t]his most recent revelation [about the 2013 Data Breach]  
22 *warrants a separate follow-up* and I plan to press the company on why its cyber defenses have been so  
23 weak as to have compromised over a billion users."<sup>56</sup> Warner, the top Democrat on the Senate  
24 Intelligence Committee, described the hacks as "*deeply troubling* . . . If a breach occurs, consumers  
25  
26

27 <sup>55</sup> Nicole Perlroth, *Yahoo Says Hackers Stole Data on 500 Million Users in 2014*, N.Y. Times (Sept.  
28 22, 2016), [http://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html?\\_r=0](http://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html?_r=0).

<sup>56</sup> See <http://www.fortune.com/2016/12/15/yahoo-hacksenator>.

1 should not be first learning of it three years later . . . Prompt notification enables users to potentially  
2 limit the harm of a breach of this kind, particularly when it may have exposed authentication  
3 information such as security question answers they may have used on other sites.” Senator Warner said  
4 that “*Yahoo had a responsibility to be more forthcoming in publicly reporting this breach sooner*  
5 *than it did . . .*”

6  
7 135. On September 26, 2016, Senator Warner wrote a letter to the chair of the SEC urging the  
8 agency to evaluate whether Yahoo “fulfilled obligations to keep public and investors informed, as  
9 required by federal law”:

10 I write to you about important federal securities matters pertaining to the Yahoo breach  
11 that may have affected 500 million accounts, and the associated lack of disclosure by the  
12 company to the public.

13 Last week, it was reported that Yahoo suffered a major breach in 2014, compromising  
14 more than 500 million accounts. Press reports indicate Yahoo’s CEO, Marissa Mayer,  
15 knew of the breach as early as July of this year. *Despite the historic scale of the breach,*  
16 *however, the company failed to file a Form 8-K disclosing the breach to the public.*

17 Furthermore, Yahoo has been engaged in an effort to sell its Internet business, including  
18 the unit affected by the breach, to Verizon since at least July 25, 2016, yet Yahoo  
19 reportedly did not inform Verizon of the breach until September 20, 2016. More  
20 puzzlingly, the company noted in a proxy statement as recently as September 9, 2016  
21 that, “To the knowledge of Seller, there have not been any incidents of, or third party  
22 claims alleging, (i) Security Breaches, unauthorized access or unauthorized use of any of  
23 Seller’s or the Business Subsidiaries’ information technology systems.”

24 Disclosure is the foundation of federal securities laws, and public companies are  
25 required to disclose material events that shareholders should know about via Form 8-K  
26 within four business days. *Data security increasingly represents an issue of vital*  
27 *importance to management, customers, and shareholders, with major corporate*  
28 *liability, business continuity, and governance implications. A breach of the magnitude*  
*that Yahoo and its users suffered seems to fit squarely within the definition of a*  
*material event. Additionally, Yahoo’s September filing asserting lack of knowledge of*  
*security incidents involving its IT systems creates serious concerns about truthfulness*  
*in representations to the public.* The public ought to know what senior executives at  
Yahoo knew of the breach, and when they knew it.

1 I encourage you to investigate whether Yahoo and its senior executives fulfilled their  
 2 obligations to keep investors and the public informed, and whether the company made  
 3 complete and accurate representations about the security of its IT systems.<sup>57</sup>

4 136. On September 27, 2016, Senators Patrick Leahy, Al Franken, Elizabeth Warren, Richard  
 5 Blumenthal, Ron Wyden and Edward Markey wrote to defendant Mayer, demanding that Yahoo  
 6 explain why the 2014 Data Breach was only recently announced despite the fact that the data was stolen  
 7 years before the disclosure:

8 ***We are even more disturbed that user information was first compromised in 2014, yet***  
 9 ***the company only announced the breach last week. That means millions of***  
 10 ***American's data may have been compromised for two years. This is unacceptable.***

11 This breach is the latest in a series of data breaches that have impacted the privacy of  
 12 millions of American consumers in recent years, but it is by far the largest. Consumers  
 13 put their trust in companies when they share personal and sensitive information with  
 14 them, and they expect all possible steps be taken to protect that information.

15 In light of these troubling revelations, please answer the following questions to help  
 16 Congress and the public better understand what went wrong and how Yahoo intends to  
 17 safeguard data and protect its users, both now and in the future. We also request that  
 18 Yahoo provide a briefing to our staff on the company's investigation into the breach, its  
 19 interaction with appropriate law enforcement and national security authorities, and how  
 20 it intends to protect affected users.

- 21 1. When and how did Yahoo first learn that its users' information may have been  
 22 compromised? Please provide a timeline detailing the nature of the breach, when  
 23 and how it was discovered, when Yahoo notified law enforcement or other  
 24 government authorities about the breach, and when Yahoo notified its customers.
- 25 2. Press reports indicate the breach first occurred in 2014, but was not discovered  
 26 until August of this year. If this is accurate, how could such a large intrusion of  
 27 Yahoo's systems have gone undetected?
- 28 3. What Yahoo accounts, services, or sister sites have been affected?
4. How many total users are affected? How were these users notified?
5. What protection is Yahoo providing the 500 million Yahoo customers whose  
 identities and personal information are now compromised?
6. What steps can consumers take to best protect the information that may have been  
 compromised in the Yahoo breach?

<sup>57</sup> [https://www.warner.senate.gov/public/index.cfm/pressreleases?ContentRecord\\_id=AC6EC18E-F309-404B-BF2D-9F60CD9884E8](https://www.warner.senate.gov/public/index.cfm/pressreleases?ContentRecord_id=AC6EC18E-F309-404B-BF2D-9F60CD9884E8).



1 7. What is Yahoo doing to prevent another breach in the future? Has Yahoo changed  
2 its security protocols, and in what manner?

3 8. Did anyone in the U.S. government warn Yahoo of a possible hacking attempt by  
4 state sponsored hackers or other bad actors? When was this warning issued?<sup>58</sup>

5 137. Yahoo is currently under investigation by the SEC for taking too long to report the  
6 breaches to investors. In December 2016, the SEC propounded requests for documents on Yahoo.

7 138. In a quarterly securities filing in November 2016, Yahoo said it was “cooperating with  
8 federal, state and foreign” agencies seeking information on the 2014 breach. Those agencies include  
9 the Federal Trade Commission, the SEC, the U.S. attorney’s office in Manhattan, and “a number of  
10 State Attorneys General.”

11 139. According to John Reed Stark, a cybersecurity consultant who previously ran the SEC’s  
12 office of internet enforcement, the Yahoo case is *particularly disturbing* because “here you are talking  
13 not just about the potential for a data breach, but a deal blowing up because of a data breach.” Mr.  
14 Stark said it was highly unusual for criminal prosecutors to take an interest in any type of disclosure  
15 matters, and unheard of in the context of cyber incident disclosures: “In my 20 years at the SEC, I never  
16 referred a disclosure case to a prosecutor.”

17 140. To date, *Yahoo has not provided an explanation why the Company took years to*  
18 *disclose the data breaches* or who made the decision not to go public sooner with this information.  
19 Questions about the hacks persist to this day. It is not just the public that Defendants continue to  
20 stonewall, but U.S. Senators as well. Yahoo's representatives were supposed to meet with members of  
21 the Senate Commerce Committee on January 31, 2017. The Company abruptly canceled that meeting  
22 on January 28, 2017. Senators John Thune and Jerry Moran wrote to defendant Mayer expressing their  
23 dismay at this "last minute" cancellation. The Senators, in their letter, stated that the Company's last  
24  
25  
26

27 \_\_\_\_\_  
28 <sup>58</sup> Letter from Senators Patrick Leahy, Al Franken, Elizabeth Warren, Richard Blumenthal, Ron  
Wyden and Edward Markey, Sept. 27, 2016, <http://www.leahy.senate.gov/imo/media/doc/9-27-16%20Yahoo%20Breach%20Letter.pdf>.

1 minute cancellation “*has prompted concerns about [Yahoo's] willingness to deal with Congress with*  
2 *complete candor about [the data breaches].*” The letter stated that “[d]espite several inquiries by  
3 Committee staff seeking information about the security of Yahoo! user accounts, *company officials*  
4 *have thus far been unable to provide answers to many basic questions.*”<sup>59</sup>

5 141. More recently, Germany’s federal cyber agency lambasted Yahoo for failing to  
6 cooperate with the agency’s investigation into the hacking probes. The agency decided to publicly  
7 report Yahoo’s stonewalling after Yahoo repeatedly refused to respond to efforts to analyze the data  
8 breaches and to prevent similar steps.<sup>60</sup>

### 10 **The Breaches Jeopardized Yahoo’s Transaction with Verizon**

11 142. According to a September 26, 2016 New York Post article published soon after Yahoo  
12 disclosed the 2014 Data Breach, “Verizon is livid they were not informed [of the breach] during due  
13 diligence and in-fighting . . . is impacting the Yahoo deal and this could be the escape clause.” The  
14 New York Post also reported that “[m]edia and tech bankers are already whispering that Verizon wants  
15 to get out of the Yahoo deal — and if they do they may pursue Twitter, which is now in play.” The  
16 Post further reported that a source said that Verizon “would expect a price renegotiation at a  
17 minimum[.]”<sup>61</sup> The scope of the hack and its potential fallout, including the possibility of costly class-  
18 action lawsuits, reportedly prompted Verizon’s renewed scrutiny of the deal. In a statement, Verizon  
19 said it would evaluate the situation “as the investigation continues through the lens of overall Verizon  
20 interests, including consumers, customers, shareholders and related communities.”  
21  
22  
23

24 \_\_\_\_\_  
25 <sup>59</sup> Robert McMillan, *Senators Question Yahoo's Candor on Data Breach*, Wall St. J. (Feb. 13, 2017,  
26 9:41 a.m.). <https://www.wsj.com/articles/senators-question-yahoos-candor-on-data-breach-1486788867>.

27 <sup>60</sup> *German cyber agency chides Yahoo for not helping in hacking probes*, Business Recorder, May 15,  
2017.

28 <sup>61</sup> See <http://www.nypost.com/2016/09/26/yahoo-hack-may-send-verizon-running-from-potential-merger>.

1 143. “If I were in Verizon’s boardroom I’d be very worried. You have to go back into every  
2 single assumption behind the valuation and redo it,” said Paul Heugh, chief executive of M&A  
3 consultancy Skarbek Associates.

4 144. “Naturally such a breach will cause concern at board level for those involved in the  
5 M&A process and eventual purchase of Yahoo,” said Richard Cassidy, UK cyber security expert at  
6 Alert Logic, a security technology company. “Questions need to be answered on why external  
7 communication has been withheld for so long.”  
8

9 145. On October 13, 2016, Bloomberg reported that Verizon’s general counsel said there was  
10 a “reasonable basis” to believe the Yahoo email breach had a material impact on the deal and that it  
11 could allow Verizon to withdraw from the agreement.  
12

13 146. The Wall Street Journal published an article on December 14, 2016 titled “Yahoo  
14 Discloses New Breach of 1 Billion User Accounts,” which indicated that the disclosure of the 2013  
15 Data Breach would further jeopardize the Verizon acquisition, and revealed that Verizon learned of the  
16 2013 Data Breach just a short time before it was publicly announced:  
17

18 The new disclosure could jeopardize Verizon’s \$4.83 billion acquisition of Yahoo’s core  
19 internet business, a deal announced in July and expected to close in early 2017. In  
20 October, Verizon signaled it could consider the 2014 breach a material event that could  
21 allow it to change the deal terms.

22 The companies were discussing the impact of that first breach when the second was  
23 discovered. Verizon learned of the latest breach in the past few weeks, a person familiar  
24 with the matter said. The company still has all options on the table, including  
25 renegotiating the deal’s price or walking away, the person said.

26 147. Analysts highlighted that “Verizon has a fiduciary duty to its shareholders to at least  
27 demand a discount on the acquisition price,” or it risks an “ignominious write off not unlike that  
28 suffered by HP after its acquisition of Autonomy.” Indeed, as of the fourth quarter of 2015, Yahoo had  
taken a \$4.46 billion “goodwill impairment charge.”

1 148. Reports indicate that the 2013 Data Breach was the largest data breach from a single site  
2 in history, more than double the size and scope of the 2014 Data Breach, which at the time it was  
3 announced had been the largest such breach.

4 149. As the result of the data breaches, Verizon, which was poised to acquire Yahoo for \$4.83  
5 billion, demanded a \$925 million discount.

6 150. More recently, a Wall Street Journal article published on February 15, 2017, reported  
7 that as a result of the data breaches, Verizon is substantially revising the terms of the deal. In  
8 particular, Verizon is cutting the cost of acquiring Yahoo's core business by approximately \$300  
9 million. Moreover, Verizon and Yahoo will now share in the payment of any future liabilities that arise  
10 from the data breaches.  
11

12 151. On February 20, 2017, Yahoo and Verizon amended the Stock Purchase Agreement,  
13 reducing the consideration to be paid by Verizon to Yahoo by \$350 million to \$4.4 billion, and  
14 providing that Yahoo and Verizon will now each be responsible for 50 percent of certain post-closing  
15 cash liabilities related to certain data security incidents and other data breaches incurred by the  
16 Company.  
17

### 18 **Yahoo Faces Significant Financial Exposure and Reputational Harm**

19 152. In the wake of the data breaches, Yahoo has disabled automatic email forwarding,  
20 preventing users who want to leave because of the recent hacking revelations from being able to switch  
21 to a rival service. Yahoo has reported that it is "work[ing] to improve" its email forwarding service, but  
22 information technology experts note that "[t]his is all extremely suspicious timing," especially given  
23 that email forwarding has been a service available to Yahoo users for over a decade and only now, and  
24 only at Yahoo, is it "under development."<sup>62</sup>  
25  
26

27 <sup>62</sup> See Associated Press, *Amid Hacking and Data Breach, Some Yahoo Users Finding it Hard to Exit*  
28 (Oct. 11, 2016), <http://www.indianexpress.com/article/technology/tech-newstechnology/amid-hacking-and-data-breach-some-yahoo-users-finding-it-hard-to-exit>.

1 153. Yahoo is facing an onslaught of government investigations. Moreover, as of the  
2 Company's most recent quarterly filing, approximately 43 consumer class actions have been filed  
3 against Yahoo thus far in U.S. federal and state courts, and foreign courts. Victimized Yahoo  
4 customers have experienced concrete harms as a result of the data breaches, including theft of monthly  
5 disability allowance; harassment by debt collection agencies for debt illicitly incurred; phishing emails;  
6 compromised tax returns and tax fraud; business penalties; fraudulent charges on personal and business  
7 cards; fraudulently opened bank accounts; hacking of personal phone lines; and receipts of  
8 pornographic emails. *See, e.g., In re Yahoo! Inc. Customer Data Breach Security Litig.*, 16-md-02752  
9 (LHK) (N.D. Cal. April 12, 2017), Dkt. No. 80.  
10

11 154. These actions and investigations subject Yahoo to significant financial exposure and  
12 reputational damage.  
13

#### 14 **Materially False and Misleading Statements Issued During the Class Period**

15 155. During the Class Period, Defendants made false and/or misleading statements and/or  
16 failed to disclose the following adverse facts pertaining to the Company's business and operations,  
17 which were known to Defendants or recklessly disregarded by them: (i) Yahoo's information security  
18 protocols were inadequate; (ii) Yahoo failed to encrypt its users' personal information and/or failed to  
19 encrypt its users' personal data with an up-to-date and secure encryption scheme, and consequently,  
20 sensitive personal account information from millions of Yahoo users was readily vulnerable to theft;  
21 (iii) as a result of Yahoo's failure to implement appropriate security measures, a massive data breach  
22 occurred in 2013, compromising the Private Information of Yahoo's users; (iv) as a result of Yahoo's  
23 failure to implement appropriate security measures, a massive data breach occurred in 2014,  
24 compromising the Private Information of Yahoo's users; (v) as a result of Yahoo's failure to implement  
25 appropriate security measures, millions of Yahoo users were victims of a forged cookie data breach in  
26 2015; (vi) as a result of Yahoo's failure to implement appropriate security measures, millions of Yahoo  
27  
28

1 users were victims of a forged cookie data breach in 2016; (vii) in contravention of SEC requirements  
 2 and the Company's own policies, Yahoo failed to disclose that a massive data breach occurred in 2013;  
 3 (viii) in contravention of SEC requirements and the Company's own policies, Yahoo failed to disclose  
 4 that a massive data breach occurred in 2014; (ix) in contravention of SEC requirements and the  
 5 Company's own policies, Yahoo failed to disclose that a forged cookie data breach exposed the private  
 6 accounts of millions of Yahoo users in 2015; (x) in contravention of SEC requirements and the  
 7 Company's own policies, Yahoo failed to disclose that a forged cookie data breach exposed the private  
 8 accounts of millions of Yahoo users in 2016; and (xi) instead of protecting its customers, Yahoo was  
 9 endangering their Private Information by failing to disclose the data breach(es).  
 10

11 **A. False and Misleading Statements Made in 2013**

12 156. On or around April 30, 2013, Yahoo made the following public representations as part of  
 13 its Privacy Policy, which the Company made available on its official website:<sup>63</sup>  
 14

15 Yahoo! takes your privacy seriously . . . We limit access to personal information about you to  
 16 employees who we believe reasonably need to come into contact with that information to  
 17 provide services to you or in order to do their jobs. We have physical, electronic, and  
 18 procedural safeguards that comply with federal regulations to protect personal information about  
 19 you.

20 157. The statements referenced in ¶ 156 above were materially false and/or misleading for the  
 21 reasons set forth in ¶ 155 (i)-(ii), (vii) and (xi) above.

22 158. On May 7, 2013, Yahoo filed a Quarterly Report on Form 10-Q with the SEC (the "Q1  
 23 2013 10-Q"). The Q1 2013 10-Q disclosed the following with respect to risks of data breaches:

24 If our security measures are breached, our products and services may be perceived as not  
 25 being secure, users and customers may curtail or stop using our products and services,  
 26 and we may incur significant legal and financial exposure.

27 <sup>63</sup> Yahoo represented that its Privacy Policy "covers how Yahoo treats personal information that  
 28 Yahoo collects and receives, including information related to your past use of Yahoo products and  
 services. Personal information is information about you that is personally identifiable like your name,  
 address, email address, or phone number, and that is not otherwise publicly available."

1 Our products and services involve the storage and transmission of Yahoo!'s users' and  
2 customers' personal and proprietary information in our facilities and on our equipment,  
3 networks and corporate systems. Security breaches expose us to a risk of loss of this  
4 information, litigation, remediation costs, increased costs for security measures, loss of  
5 revenue, damage to our reputation, and potential liability. Our user data and corporate  
6 systems and security measures have been and may in the future be breached due to the  
7 actions of outside parties (including cyber attacks), employee error, malfeasance, a  
8 combination of these, or otherwise, allowing an unauthorized party to obtain access to  
9 our data or our users' or customers' data. Additionally, outside parties may attempt to  
10 fraudulently induce employees, users, or customers to disclose sensitive information in  
11 order to gain access to our data or our users' or customers' data.

12 Any breach or unauthorized access could result in significant legal and financial  
13 exposure, increased remediation and other costs, damage to our reputation and a loss of  
14 confidence in the security of our products, services and networks that could potentially  
15 have an adverse effect on our business. Because the techniques used to obtain  
16 unauthorized access, disable or degrade service, or sabotage systems change frequently  
17 or may be designed to remain dormant until a predetermined event and often are not  
18 recognized until launched against a target, we may be unable to anticipate these  
19 techniques or implement adequate preventative measures. If an actual or perceived  
20 breach of our security occurs, the market perception of the effectiveness of our security  
21 measures could be harmed and we could lose users and customers.

22 159. The Q1 2013 10-Q contained signed certifications pursuant to SOX by Defendant  
23 Mayer, stating that the financial information contained in the Q1 2013 10-Q was accurate.

24 160. The statements referenced in ¶ 158 above were materially false and/or misleading for the  
25 reasons set forth in ¶ 155 (i)-(ii), (vii) and (xi) above.

26 161. On August 8, 2013, Yahoo filed another Quarterly Report on Form 10-Q with the SEC  
27 (the "Q2 2013 10-Q"). The Q2 2013 10-Q disclosed the following with respect to risks of data  
28 breaches:

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. Our user data and corporate  
systems and security measures have been and may in the future be breached due to the  
actions of outside parties (including cyber attacks), employee error, malfeasance, a  
combination of these, or otherwise, allowing an unauthorized party to obtain access to

1 our data or our users' or customers' data. Additionally, outside parties may attempt to  
2 fraudulently induce employees, users, or customers to disclose sensitive information in  
order to gain access to our data or our users' or customers' data.

3 Any breach or unauthorized access could result in significant legal and financial  
4 exposure, increased remediation and other costs, damage to our reputation and a loss of  
5 confidence in the security of our products, services and networks that could potentially  
6 have an adverse effect on our business. Because the techniques used to obtain  
7 unauthorized access, disable or degrade service, or sabotage systems change frequently  
8 or may be designed to remain dormant until a predetermined event and often are not  
recognized until launched against a target, we may be unable to anticipate these  
9 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.

9 162. The Q2 2013 10-Q contained signed certifications pursuant to SOX by Defendant  
10 Mayer, stating that the financial information contained in the Q2 2013 10-Q was accurate.

11 163. The statements referenced in ¶ 161 above were materially false and/or misleading for the  
12 reasons set forth in ¶ 155 (i)-(iii), (vii) and (xi) above.

13 164. On September 6, 2013, Yahoo posted on its official website the following statement  
14 from Ronald Bell, Yahoo's General Counsel: "At Yahoo, we take the privacy of our users seriously."

15 165. The statement referenced in ¶ 164 above was materially false and/or misleading for the  
16 reasons set forth in ¶ 155 (i)-(iii), (vii) and (xi) above.

17 166. On October 14, 2013, Yahoo posted on its official website the following statements from  
18 Jeffrey Bonforte, SVP of Communication Products, concerning Yahoo's commitment to the security of  
19 its customers:  
20  
21

22 At Yahoo, we take the security of our users very seriously. In a constantly changing  
23 digital environment, we recognize the need to continuously evaluate how to best protect  
your information.

24 Yahoo Mail users can already enable https [or Secure Sockets Layer (SSL)], a  
25 communications protocol that securely encrypts your information and messages as they  
26 move between your browser and Yahoo's servers. You'll find this option in your Yahoo  
Mail settings menu under the security tab. Electing this option enhances your privacy  
27 and security.



1 167. On that day, Yahoo also posted on its official website the following additional  
2 statements by Bonforte:

3 Starting January 8, 2014, we will make encrypted https connections standard for all  
4 Yahoo Mail users. Our teams are working hard to make the necessary changes to default  
5 https connections on Yahoo Mail, and we look forward to providing this extra layer of  
6 security for all our users.

7 Yahoo will continue to enhance our security technology, policies and practices to  
8 provide the best possible protections for our users. We invite you to check out our  
9 Yahoo Security Center to learn about other steps you can take to help protect yourself  
10 online.

11 UPDATE:

12 In addition to making https a default feature by January 2014 for all Yahoo Mail users,  
13 we plan to implement 2048-bit encryption keys, which will provide our users with a  
14 further layer of security.

15 168. The statements referenced in ¶¶ 166-67 above were materially false and/or misleading  
16 for the reasons set forth in ¶ 155 (i)-(iii), (vii) and (xi) above.

17 169. On November 12, 2013, Yahoo filed a Quarterly Report on Form 10-Q with the SEC  
18 (the “Q3 2013 10-Q”). The Q3 2013 10-Q disclosed the following with respect to risks of data  
19 breaches:

20 If our security measures are breached, our products and services may be perceived as not  
21 being secure, users and customers may curtail or stop using our products and services,  
22 and we may incur significant legal and financial exposure.

23 Our products and services involve the storage and transmission of Yahoo’s users’ and  
24 customers’ personal and proprietary information in our facilities and on our equipment,  
25 networks and corporate systems. Security breaches expose us to a risk of loss of this  
26 information, litigation, remediation costs, increased costs for security measures, loss of  
27 revenue, damage to our reputation, and potential liability. Our user data and corporate  
28 systems and security measures have been and may in the future be breached due to the  
actions of outside parties (including cyber attacks), employee error, malfeasance, a  
combination of these, or otherwise, allowing an unauthorized party to obtain access to  
our data or our users’ or customers’ data. Additionally, outside parties may attempt to  
fraudulently induce employees, users, or customers to disclose sensitive information in  
order to gain access to our data or our users’ or customers’ data.

Any breach or unauthorized access could result in 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 potentially  
have an adverse effect on our business. Because the techniques used to obtain

1 unauthorized access, disable or degrade service, or sabotage systems change frequently  
2 or may be designed to remain dormant until a predetermined event and often are not  
3 recognized until launched against a target, we may be unable to anticipate these  
4 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.

5 170. The Q3 2013 10-Q contained signed certifications pursuant to the Sarbanes-Oxley Act of  
6 2002 (“SOX”) by Defendant Mayer, stating that the financial information contained in the Q3 2013 10-  
7 Q was accurate.

8 171. The statements referenced in ¶ 169 above were materially false and/or misleading for the  
9 reasons set forth in ¶ 155 (i)-(iii), (vii) and (xi) above.

10 172. On November 18, 2013, Yahoo posted on its official website the following statements  
11 made by Defendant Mayer, concerning Yahoo’s commitment to protecting the personal information of  
12 its customers:  
13

14 We’ve worked hard over the years to earn our users’ trust and we fight hard to preserve  
15 it . . .

16 There is nothing more important to us than protecting our users’ privacy. To that end, we  
17 recently announced that we will make Yahoo Mail even more secure by introducing  
18 https (SSL - Secure Sockets Layer) encryption with a 2048-bit key across our network  
by January 8, 2014.

19 Today we are announcing that we will extend that effort across all Yahoo products.  
More specifically this means we will:

- 20 ○ Encrypt all information that moves between our data centers by the end of Q1  
21 2014;
- 22 ○ Offer users an option to encrypt all data flow to/from Yahoo by the end of Q1  
23 2014;
- 24 ○ Work closely with our international Mail partners to ensure that Yahoo co-  
25 branded Mail accounts are https-enabled.

26 As we have said before, we will continue to evaluate how we can protect our users’  
27 privacy and their data. We appreciate, and certainly do not take for granted, the trust our  
28 users place in us.

173. The statements referenced in ¶ 172 above were materially false and/or misleading for the  
reasons set forth in ¶ 155 (i)-(iii), (vii) and (xi) above.

1 174. On the same date, Defendant Mayer reinforced in her Twitter and Tumblr accounts  
2 “Yahoo’s commitment to securing and encrypting (...) users’ data.”

3 175. The statement referenced in ¶ 174 above was materially false and/or misleading for the  
4 reasons set forth in ¶ 155 (i)-(iii), (vii) and (xi) above.

5 **B. False and Misleading Statements Made in 2014**

6 176. On January 7, 2014, Yahoo posted on its official website the following statement from  
7 Jeffrey Bonforte:

8  
9 Yahoo is fully committed to keeping our users safe and secure online. As we promised  
10 back in October, we are now automatically encrypting all connections between our users  
11 and Yahoo Mail. Anytime you use Yahoo Mail - whether it’s on the web, mobile web,  
12 mobile apps, or via IMAP, POP or SMTP- it is 100% encrypted by default and protected  
with 2,048 bit certificates. This encryption extends to your emails, attachments, contacts,  
as well as Calendar and Messenger in Mail.

13 Security is a key focus for us and we’ll continue to enhance our security technology and  
14 policies so we can provide a safe and secure experience for our users.

15 177. The statements referenced in ¶ 176 above were materially false and/or misleading for the  
16 reasons set forth in ¶ 155 (i)-(iv), (vii)-(viii), and (xi) above.

17 178. At Yahoo’s January 28, 2014 Earnings Call for the fourth quarter of 2013, Defendant  
18 Mayer represented that “in the beginning of January, Yahoo! Mail turned on SSL secure protocol for  
19 100% of users. And the SSL protocol applies to ads as well, effectively making us the largest secure  
20 publisher on the web utilizing display advertising.”

21 179. The statements referenced in ¶ 178 above were materially false and/or misleading for the  
22 reasons set forth in ¶ 155 (i)-(iv), (vii)-(viii), and (xi) above.

23 180. On February 28, 2014, Yahoo filed an Annual Report on Form 10-K with the SEC (the  
24 “2013 10-K”). The 2013 10-K disclosed the following with respect to risks of data breaches:

25  
26 If our security measures are breached, our products and services may be perceived as not  
27 being secure, users and customers may curtail or stop using our products and services,  
28 and we may incur significant legal and financial exposure.

1 Our products and services involve the storage and transmission of Yahoo's users' and  
2 customers' personal and proprietary information in our facilities and on our equipment,  
3 networks and corporate systems. Security breaches expose us to a risk of loss of this  
4 information, litigation, remediation costs, increased costs for security measures, loss of  
5 revenue, damage to our reputation, and potential liability. Security breaches or  
6 unauthorized access have resulted in and may in the future result in a combination of  
7 significant legal and financial exposure, increased remediation and other costs, damage  
8 to our reputation and a loss of confidence in the security of our products, services and  
9 networks that could have an adverse effect on our business. We take steps to prevent  
10 unauthorized access to our corporate systems, however, because the techniques used to  
11 obtain unauthorized access, disable or degrade service, or sabotage systems change  
12 frequently or may be designed to remain dormant until a triggering event, we may be  
13 unable to anticipate these techniques or implement adequate preventative measures. If an  
14 actual or perceived breach of our security occurs, the market perception of the  
15 effectiveness of our security measures could be harmed and we could lose users and  
16 customers.

17 181. The 2013 10-K contained signed certifications pursuant to SOX by Defendant Mayer,  
18 stating that the financial information contained in the 2013 10-K was accurate.

19 182. The statements referenced in ¶ 180 above were materially false and/or misleading for the  
20 reasons set forth in ¶ 155 (i)-(iv), (vii)-(viii), and (xi) above.

21 183. On March 14, 2014, Defendant Bell was quoted in the Silicon Valley Business Journal  
22 stating that "I have a real sense, and everyone in the legal department thinks that our main job is to  
23 protect our users. We have to stand up for them, because if we don't, nobody else is in a position to do  
24 that."

25 184. The Silicon Valley Business Journal enjoys wide public circulation and covers the latest  
26 news for professionals and others, including technology news, both online and in print. It also hosts a  
27 number of panels, events and awards presentations that are informative in nature. In addition to its  
28 subscribers, the Silicon Valley Business Journal's Facebook account has over 28,000 followers; its  
Twitter account has over 20,000 followers; and its LinkedIn account has over 3,500 followers.

185. The statements referenced in ¶ 183 above were materially false and/or misleading for the  
reasons set forth in ¶ 155 (i)-(iv), (vii)-(viii), and (xi) above.

1 186. On April 2, 2014, Yahoo posted on its official website the following statements from  
2 Alex Stamos, Yahoo's Chief Information Security Officer:

3 When I joined Yahoo four weeks ago, we were in the middle of a massive project to  
4 protect our users and their data through the deployment of encryption technologies as we  
discussed in our November 2013 Tumblr.

5 So today, we're updating you on our progress:

6 Traffic moving between Yahoo data centers is fully encrypted as of March 31.

7 In January, we made Yahoo Mail more secure by making browsing over HTTPS the  
8 default. In the last month, we enabled encryption of mail between our servers and other  
mail providers that support the SMTPTLS standard.

9 The Yahoo Homepage and all search queries that run on the Yahoo Homepage and most  
10 Yahoo properties also have HTTPS encryption enabled by default.

11 We implemented the latest in security best-practices, including supporting TLS 1.2,  
12 Perfect Forward Secrecy and a 2048-bit RSA key for many of our global properties such  
as Homepage, Mail and Digital Magazines. We are currently working to bring all Yahoo  
sites up to this standard.

13 187. Yahoo also posted on its official website the following statements by Alex Stamos on  
14 April 2, 2014, with respect to Yahoo's continued commitments to improving its security:

15 Hundreds of Yahoos have been working around the clock over the last several months to  
16 provide a more secure experience for our users and we want to do even more moving  
17 forward. Our goal is to encrypt our entire platform for all users at all time, by default.

18 One of our biggest areas of focus in the coming months is to work with and encourage  
19 thousands of our partners across all of Yahoo's hundreds of global properties to make  
sure that any data that is running on our network is secure. Our broader mission is to not  
20 only make Yahoo secure, but improve the security of the overall web ecosystem.

21 In addition to moving all of our properties to encryption by default, we will be  
22 implementing additional security measures such as HSTS, Perfect Forward Secrecy and  
23 Certificate Transparency over the coming months. This isn't a project where we'll ever  
check a box and be "finished." Our fight to protect our users and their data is an on-  
24 going and critical effort. We will continue to work hard to deploy the best possible  
technology to combat attacks and surveillance that violate our users' privacy.

25 188. The statements referenced in ¶¶ 186-87 above were materially false and/or misleading  
26 for the reasons set forth in ¶ 155 (i)-(iv), (vii)-(viii), and (xi) above.

27 189. On April 11, 2014, Yahoo posted on its official website the following statements from  
28 Jeffrey Bonforte:

1 The world has changed. So while email is an essential tool for business and personal life,  
2 it is also the focus for some of those who endeavor to do us harm. The new normal  
3 across the web can include massive attempts at account hacking, email spoofing (forging  
4 sender identity) and phishing attacks (tricking a user to give up account credentials).

5 The doors to your inbox need another lock.

6 Because of the rise of spoofing and phishing attacks, the industry saw a need over two  
7 years ago to require emails to be sent more securely and formed an organization,  
8 including Yahoo, Google, Aol, Microsoft, LinkedIn, and Facebook, to work out a  
9 solution. The organization designed and built something called DMARC, or Domain-  
10 based Message Authentication, Reporting and Conformance. Today, 80% of US email  
11 user accounts and over 2B accounts globally can be protected by the DMARC standard.

12 On Friday afternoon last week, Yahoo made a simple change to its DMARC policy from  
13 “report” to “reject”. In other words, we requested that all other mail services reject  
14 emails claiming to come from a Yahoo user, but not signed by Yahoo.

15 Yahoo is the first major email provider in the world to adopt this aggressive level of  
16 DMARC policy on behalf of our users.

17 And overnight, the bad guys who have used email spoofing to forge emails and launch  
18 phishing attempts pretending to come from a Yahoo Mail account were nearly stopped in  
19 their tracks . . .

20 With stricter DMARC policies, users are safer, and the bad guys will be in a tough spot.  
21 More importantly, verified senders will unlock a massive wave of innovation and  
22 advancement for all our inboxes.

23 190. The statements referenced in ¶ 189 above were materially false and/or misleading for the  
24 reasons set forth in ¶ 155 (i)-(iv), (vii)-(viii), and (xi) above.

25 191. At Yahoo’s April 15, 2014 Earnings Call for the first quarter of 2014, Defendant Mayer  
26 praised Yahoo’s retention of Alex Stamos as the Company’s VP of Information Security to strengthen  
27 security: “Alex Stamos joined Yahoo! as VP of Information Security. Alex brings vast information  
28 security experience to Yahoo! and will be on the front line of continuing to ensure that our products are  
as secure as possible. He will be furthering our significant security efforts to date, especially around  
enabling SSL as a preferred option across our offerings.”

192. The statements referenced in ¶ 191 above were materially false and/or misleading for the  
reasons set forth in ¶ 155 (i)-(iv), (vii)-(viii), and (xi) above.

1 193. On May 8, 2014, Yahoo filed a Quarterly Report on Form 10-Q with the SEC (the “Q1  
2 2014 10-Q”). The Q1 2014 10-Q disclosed the following with respect to risks of data breaches:

3 If our security measures are breached, our products and services may be perceived as not  
4 being secure, users and customers may curtail or stop using our products and services,  
5 and we may incur significant legal and financial exposure.

6 Our products and services involve the storage and transmission of Yahoo’s users’ and  
7 customers’ personal and proprietary information in our facilities and on our equipment,  
8 networks and corporate systems. Security breaches expose us to a risk of loss of this  
9 information, litigation, remediation costs, increased costs for security measures, loss of  
10 revenue, damage to our reputation, and potential liability. Security breaches or  
11 unauthorized access have resulted in and may in the future result in a combination of  
12 significant legal and financial exposure, increased remediation and other costs, damage  
13 to our reputation and a loss of confidence in the security of our products, services and  
14 networks that could have an adverse effect on our business. We take steps to prevent  
15 unauthorized access to our corporate systems, however, because the techniques used to  
16 obtain unauthorized access, disable or degrade service, or sabotage systems change  
17 frequently or may be designed to remain dormant until a triggering event, we may be  
18 unable to anticipate these techniques or implement adequate preventative measures. If an  
19 actual or perceived breach of our security occurs, the market perception of the  
20 effectiveness of our security measures could be harmed and we could lose users and  
21 customers.

22 194. The Q1 2014 10-Q contained signed certifications pursuant to SOX by Defendant  
23 Mayer, stating that the financial information contained in the Q1 2014 10-Q was accurate.

24 195. The statements referenced in ¶ 193 above were materially false and/or misleading for the  
25 reasons set forth in ¶ 155 (i)-(iv), (vii)-(viii), and (xi) above.

26 196. On May 15, 2014, Yahoo posted on its official website the following statements from  
27 Alex Stamos, about Yahoo’s ongoing commitments to put its “users first”:

28 The Senate Homeland Security and Government Affairs Permanent Subcommittee on  
Investigations hosted a hearing earlier today to examine consumer security and data  
privacy in the online advertising industry. I testified along with representatives from  
Google and the Online Trust Alliance. *I focused on Yahoo’s dedication to protecting  
our users and you can download my written testimony here* (scroll down to “Panel  
One”).

This hearing gave us the opportunity to discuss the *user-first approach to security we  
take at Yahoo. We build and maintain user trust by providing secure product  
experiences for all of our users across the globe. Because we never take the*

1 *relationship we've cultivated with our users for granted, 800 million people each*  
2 *month trust us to provide them with Internet services across mobile and web.*

3 *I outlined specific ways we protect our users, including: our focus on security in the*  
4 *advertising pipeline; our leadership in the fight on email spam; the bug bounty*  
5 *program we operate; and our efforts to fully encrypt 100 percent of our network*  
6 *traffic.*

7 Achieving security online is not an end state; it's a constantly evolving **challenge** that  
8 **we tackle head on**. At Yahoo, we know that our users rely on us to help protect their  
9 information for them. We also see security as a partnership - we want to educate our  
10 users to be mindful of their own security habits, and we provide intuitive, user-friendly  
11 tools and security resources to help them do so.

12 197. Yahoo's official website included a link to Mr. Stamos' testimony, which addressed the  
13 topic of Yahoo's users-first approach to security:

14 One reason I joined Yahoo is that from the top down, the company is devoted to  
15 protecting users. Building and maintaining trust through secure products is a critical  
16 focus for us, and by default all of our products should be secure for all of our users  
17 across the globe.

18 Achieving security online is not an end state; it's a constantly evolving challenge that we  
19 tackle head on. At Yahoo, we know that our users rely on us to protect their information.  
20 We also see security as a partnership; we want to educate our users to be mindful of their  
21 own security habits, and we provide intuitive, user-friendly tools and security resources  
22 to help them do so.

23 Malware is an important issue that is a top priority for Yahoo. While distribution of  
24 malware through advertising is one part of the equation, it's important to address the  
25 entire malware ecosystem and fight it at each phase of its lifecycle. It is also important to  
26 address security more broadly across the Internet.

27 I outline in my testimony below several specific ways Yahoo is fighting criminals and  
28 protecting our users, including: focusing on security in the advertising pipeline and  
sharing threats; leading the fight on email spam; operating a bug bounty program; and  
working to fully encrypt 100 percent of Yahoo's network traffic.

198. Mr. Stamos outlined the steps taken by Yahoo against malware and deceptive ads.  
Yahoo posted this information on its official website:

We successfully block the vast majority of malicious or deceptive advertisements with  
which bad actors attack our network, and we always strive to defeat those who would  
compromise our customers' security. This means we regularly improve our systems,  
including continuously diversifying the set of technologies and testing systems to better  
emulate different user behaviors. Every ad running on Yahoo's sites or on our ad  
network is inspected using this system, both when they are created and continuously  
afterward.



1 Yahoo also strives to keep deceptive advertisements from ever reaching users. For  
2 example, our systems prohibit advertisements that look like operating system messages,  
3 because such ads often tout false offers or try to trick users into downloading and  
4 installing malicious or unnecessary software. Preventing deceptive advertising once  
5 required extensive human intervention, which meant slower response times and  
6 inconsistent enforcement. Although no system is perfect, we now use sophisticated  
7 machine learning and image recognition algorithms to catch deceptive advertisements.

8 This lets us train our systems about the characteristics of deceptive creatives, advertisers  
9 and landing sites so we detect and respond to them immediately.

10 We are also the driving force behind the SafeFrame standard. The SafeFrame  
11 mechanism allows ads to properly display on a web page without exposing a user's  
12 private information to the advertiser or network. Thanks to widespread adoption,  
13 SafeFrame enhances user privacy and security not only in the thriving marketplace of  
14 thousands of publishers on Yahoo, but around the Internet.

15 199. Mr. Stamos also explained how Yahoo was "leading the fight on email spam." Yahoo  
16 posted this information on its official website:

17 While preventing the placement of malicious advertisements is essential, it is only one  
18 part of a larger battle. We also fight the rest of the malware lifecycle by improving ways  
19 to validate the authenticity of email and by reducing financial incentives to spread  
20 malware. Spam is one of the most effective ways malicious actors make money, and  
21 Yahoo is leading the fight to eradicate that source of income. For example, one way  
22 spammers act is through "email spoofing". The original Internet mail standards did not  
23 require that a sender use an accurate "From:" line in an email. Spammers exploit this to  
24 send billions of messages a day that feign to be from friends, family members or  
25 business associates. These emails are much more likely to bypass spam filters, as they  
26 appear to be from trusted correspondents. Spoofed emails can also be used to trick users  
27 into giving up usernames and passwords, a technique known generally as "phishing".

28 Yahoo is helping the Internet industry tackle these issues. Yahoo was the original author  
of DomainKeys Identified Mail or DKIM, a mechanism that lets mail recipients  
cryptographically verify the real origin of email. Yahoo freely contributed the  
intellectual property behind DKIM to the world, and now the standard protects billions  
of emails between thousands of domains. Building upon the success of DKIM, Yahoo  
led a coalition of Internet companies, financial institutions and anti-spam groups in  
creating the Domain-based Message Authentication, Reporting and Conformance or  
DMARC Standard . . . DMARC provides domains a way to tell the rest of the Internet  
what security mechanisms to expect on email they receive and what actions the sender  
would like to be taken on spoofed messages.

In April of this year, Yahoo became the first major email provider to publish a strict  
DMARC reject policy. In essence, we asked the rest of the Internet to drop messages that  
inaccurately claim to be from yahoo.com users. Since Yahoo made this change another  
major provider has enabled DMARC reject. We hope that every major email provider  
will follow our lead and implement this common sense protection against spoofed email.  
DMARC has reduced spam purported to come from yahoo.com accounts by over 90%.

1 If used broadly, it would target spammers' financial incentives with crippling  
2 effectiveness.

3 200. Mr. Stamos also touted Yahoo's protection of private information through encryption.

4 Yahoo posted this information on its official website:

5 Yahoo invests heavily to ensure the security of our users and their data across all of our  
6 products. In January, we made encrypted browsing the default for Yahoo Mail. And as  
7 of March of this year, domestic and international traffic moving between Yahoo's data  
8 centers has been fully encrypted.

9 201. The statements referenced in ¶¶ 196-200 above were materially false and/or misleading  
10 for the reasons set forth in ¶ 155 (i)-(iv), (vii)-(viii), and (xi) above.

11 202. On June 5, 2014, Yahoo posted on its official website the following statements from  
12 Ronald Bell:

13 Here's a look at how we've had our users' back when it comes to security and  
14 transparency: . . .

15 Encryption: In November 2013, we committed to introducing HTTPS (SSL - Secure  
16 Sockets Layer) encryption with 2048-bit keys across our network. We've made  
17 significant progress toward this goal, including:

18 encrypting all data moving between our data centers;

19 making browsing via Yahoo Mail HTTPS by default;

20 ensuring that the Yahoo Homepage and all search queries run on the Yahoo  
21 Homepage and most Yahoo properties have HTTPS by default;

22 implementing the latest in security best-practices, including supporting TLS 1.2,  
23 Perfect Forward Secrecy, and a 2048-bit RSA key for many of our global properties  
24 such as Homepage, Mail and Digital Magazines;

25 empowering users to initiate an encrypted session for Yahoo News, Yahoo Sports,  
26 Yahoo Finance, and Good Morning America on Yahoo (gma.yahoo.com) by typing  
27 "https" before the site URL in their web browser;

28 preparing to deploy a new, encrypted, version of Yahoo Messenger in coming  
months;

work with our thousands of partners to make sure that data running on our network is  
secure.

203. The statements referenced in ¶ 202 above were materially false and/or misleading for the  
reasons set forth in ¶ 155 (i)-(iv), (vii)-(viii), and (xi) above.

1 204. On July 25, 2014, Yahoo posted on its official website the following statements from  
2 Alex Stamos, praising two new members of the company's security team and stating that:

3 The security of our users is a huge focus for us at Yahoo. We're deploying encryption  
4 technologies across our platform, encouraging our partners to ensure that any data  
5 running on our network is secure, and improving the security of the overall web  
ecosystem.

6 205. The statements referenced in ¶ 204 above were materially false and/or misleading for the  
7 reasons set forth in ¶ 155 (i)-(iv), (vii)-(viii), and (xi) above.

8 206. On August 7, 2014, Yahoo filed a Quarterly Report on Form 10-Q with the SEC (the  
9 "Q2 2014 10-Q"). The Q2 2014 10-Q disclosed the following with respect to risks of data breaches:  
10

11 If our security measures are breached, our products and services may be perceived as not  
12 being secure, users and customers may curtail or stop using our products and services,  
and we may incur significant legal and financial exposure.

13 Our products and services involve the storage and transmission of Yahoo's users' and  
14 customers' personal and proprietary information in our facilities and on our equipment,  
15 networks and corporate systems. Security breaches expose us to a risk of loss of this  
16 information, litigation, remediation costs, increased costs for security measures, loss of  
17 revenue, damage to our reputation, and potential liability. Security breaches or  
18 unauthorized access have resulted in and may in the future result in a combination of  
19 significant legal and financial exposure, increased remediation and other costs, damage  
20 to our reputation and a loss of confidence in the security of our products, services and  
21 networks that could have an adverse effect on our business. We take steps to prevent  
22 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.

23 207. The Q2 2014 10-Q contained signed certifications pursuant to SOX by Defendant  
24 Mayer, stating that the financial information contained in the Q2 2014 10-Q was accurate.

25 208. The statements referenced in ¶ 206 above were materially false and/or misleading for the  
26 reasons set forth in ¶ 155 (i)-(iv), (vii)-(viii), and (xi) above.  
27  
28

1           209. On August 7, 2014, in a presentation made by Alex Stamos on behalf of Yahoo at the  
2 Black Hat USA 2014 conference, the world’s leading information security event, Yahoo pointed out  
3 how the Company combats security bugs:

- 4           • Detailed descriptions and mitigation instructions
- 5           • Accurate prioritization
- 6           • Consistent follow-up and real-time reporting
- 7           • Executive visibility
- 8           • Convincing company that you are a madman

9           210. At this event, Alex Stamos highlighted that “something that works really well for  
10 [Yahoo] is that the leaders of all our business units have a real-time dashboard to see how many bugs  
11 are handing over them and our CEO every week confronts that number.”

12           211. The statements referenced in ¶¶ 209-10 above were materially false and/or misleading  
13 for the reasons set forth in ¶ 155 (i)-(iv), (vii)-(viii), and (xi) above.

14           212. On September 11, 2014, Yahoo posted on its official website the following statements  
15 from Ronald Bell: “Users come first at Yahoo . . . We are also committed to protecting users’ data.”

16           213. The statements referenced in ¶ 212 above were materially false and/or misleading for the  
17 reasons set forth in ¶ 155 (i)-(iv), (vii)-(viii), and (xi) above.

18           214. On September 25, 2014, Yahoo made the following public representations as part of its  
19 Privacy Policy, which the Company posted on its official website:  
20

21           Yahoo! takes your privacy seriously . . .

22           We limit access to personal information about you to employees who we believe  
23 reasonably need to come into contact with that information to provide products or  
24 services to you or in order to do their jobs.

25           We have physical, electronic, and procedural safeguards that comply with federal  
26 regulations to protect personal information about you.

27           215. With respect to Information Sharing and Disclosure, Yahoo’s Privacy Policy made the  
28 following representations:

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

4 We provide the information to trusted partners who work on behalf of or with  
5 Yahoo under confidentiality agreements. These companies may use your  
6 personal information to help Yahoo communicate with you about offers from  
7 Yahoo and our marketing partners. However, these companies do not have any  
8 independent right to share this information.

9 We have a parent's permission to share the information if the user is a child  
10 under age 13.

11 We respond to subpoenas, court orders, or legal process (such as law  
12 enforcement requests), or to establish or exercise our legal rights or defend  
13 against legal claims.

14 We believe it is necessary to share information in order to investigate, prevent, or  
15 take action regarding illegal activities, suspected fraud, situations involving  
16 potential threats to the physical safety of any person, violations of Yahoo's terms  
17 of use, or as otherwise required by law.

18 We transfer information about you if Yahoo is acquired by or merged with  
19 another company. In this event, Yahoo will notify you before information about  
20 you is transferred and becomes subject to a different privacy policy.

21 216. In the 2014 Privacy Policy, Yahoo also disclosed the following information about  
22 specific steps it was taking to further detect and defend fraudulent activity:

23 Updated to include data collection practices-Data Storage and Anonymization link:

24 In addition to the other purposes for which we collect information, other types of log  
25 data (ie not relating to search) (such as ad views, ad clicks, page views and page clicks)  
26 are retained for a longer period in order to power innovative product development,  
27 provide personalized and customized services, and better able our security systems to  
28 detect and defend against fraudulent activity.

Q: What is Yahoo's updated user log data retention policy?

A: Yahoo's new policy will be able to de-identify search log data within 18 months of  
collection with limited exceptions to meet legal obligations. For other, non-search log  
data we collect, that data will be retained for a longer period in order to power  
innovative product development, provide personalized experiences, and better enable our  
security systems to detect and defend against fraudulent activity.

217. The statements referenced in ¶¶ 214-16 above were materially false and/or misleading  
for the reasons set forth in ¶ 155 (i)-(iv), (vii)-(viii), and (xi) above.

1 218. On October 6, 2014, Yahoo posted on its official website another statement from Alex  
2 Stamos, affirming that “[the company] remains committed to providing the most secure experience  
3 possible for [its] users worldwide.”

4 219. The statement referenced in ¶ 218 above was materially false and/or misleading for the  
5 reasons set forth in ¶ 155 (i)-(iv), (vii)-(viii), and (xi) above.

6 220. On November 7, 2014, Yahoo filed a Quarterly Report on Form 10-Q with the SEC (the  
7 “Q3 2014 10-Q”). The Q3 2014 10-Q disclosed the following with respect to risks of data breaches:  
8

9 If our security measures are breached, our products and services may be perceived as not  
10 being secure, users and customers may curtail or stop using our products and services,  
and we may incur significant legal and financial exposure.

11 Our products and services involve the storage and transmission of Yahoo’s users’ and  
12 customers’ personal and proprietary information in our facilities and on our equipment,  
13 networks and corporate systems. Security breaches expose us to a risk of loss of this  
14 information, litigation, remediation costs, increased costs for security measures, loss of  
15 revenue, damage to our reputation, and potential liability. Security breaches or  
16 unauthorized access have resulted in and may in the future result in a combination of  
17 significant legal and financial exposure, increased remediation and other costs, damage  
18 to our reputation and a loss of confidence in the security of our products, services and  
19 networks that could have an adverse effect on our business. We take steps to prevent  
20 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.

21 221. The Q3 2014 10-Q contained signed certifications pursuant to SOX by Defendant  
22 Mayer, stating that the financial information contained in the Q3 2014 10-Q was accurate.

23 222. The statements referenced in ¶ 220 above were materially false and/or misleading for the  
24 reasons set forth in ¶ 155 (i)-(iv), (vii)-(viii), and (xi) above.  
25

26 **C. False and Misleading Statements Made in 2015**

27 223. On February 9, 2015, Yahoo posted on its official website the following statements from  
28 Lovlesh Chhabra, the Company’s Product Manager:

1 At Yahoo, our users' security is paramount, and we continue to update our policies and practices  
2 to keep our users' accounts and data secure. While developers and partners using Yahoo APIs  
3 are currently able to use basic authentication protocols and/or 'plain text' usernames and  
4 passwords to authenticate their users, beginning May 30, 2015, all third-party applications will  
5 need to move to OAuth-based authentication. The good news is that Yahoo APIs already  
6 support OAuth-based authentication.

7 224. The statements referenced in ¶ 223 above were materially false and/or misleading for the  
8 reasons set forth in ¶ 155 (i)-(v), (vii)-(ix), and (xi) above.

9 225. On February 27, 2015, Yahoo filed an Annual Report on Form 10-K with the SEC (the  
10 "2014 10-K"). The 2014 10-K disclosed the following with respect to risks of data breaches:

11 If our security measures are breached, our products and services may be perceived as not  
12 being secure, users and customers may curtail or stop using our products and services,  
13 and we may incur significant legal and financial exposure.

14 Our products and services involve the storage and transmission of Yahoo's users' and  
15 customers' personal and proprietary information in our facilities and on our equipment,  
16 networks and corporate systems. Security breaches expose us to a risk of loss of this  
17 information, litigation, remediation costs, increased costs for security measures, loss of  
18 revenue, damage to our reputation, and potential liability. Outside parties may attempt to  
19 fraudulently induce employees, users, or customers to disclose sensitive information to  
20 gain access to our data or our users' or customers' data. In addition, hardware, software  
21 or applications we procure from third parties may contain defects in design or  
22 manufacture or other problems that could unexpectedly compromise network and data  
23 security. Security breaches or unauthorized access have resulted in and may in the future  
24 result in a combination of significant legal and financial exposure, increased remediation  
25 and other costs, damage to our reputation and a loss of confidence in the security of our  
26 products, services and networks that could have an adverse effect on our business. We  
27 take steps to prevent unauthorized access to our corporate systems, however, because the  
28 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.

29 226. The 2014 10-K contained signed certifications pursuant to SOX by Defendant Mayer,  
30 stating that the financial information contained in the 2014 10-K was accurate.

31 227. The statements referenced in ¶ 225 above were materially false and/or misleading for the  
32 reasons set forth in ¶ 155 (i)-(v), (vii)-(ix), and (xi) above.

1 228. On March 6, 2015, at the World Economic Forum, Defendant Mayer was a guest  
2 speaker on the topic of digital technology. The speech by Defendant Mayer was made available to the  
3 public, including on the Internet. Mayer touted Yahoo's implementation of secure protocols to  
4 safeguard its customers' data:

5 Q: Given Snowden and also the counterterrorism problem at the moment, how much has  
6 that raised much more questioning about your storage of say emails, in other words, how  
7 would you say Yahoo now stands on what we might call the trust index...?

8 Mayer: . . . [T]he first thing that happened when [] we heard about Snowden's  
9 allegations is we changed the way that we store data, we changed the way that we  
10 communicate data, we went to entirely secure connections on all of the, Yahoo's major  
11 properties hgtps, we changed the way we did encryption between the data centers to  
12 basically get a more secure environment for our end users because we realized that's  
13 what they wanted. So we changed all of those things in response to those allegations.

14 Q: And what was the impact on trust?

15 Mayer: We didn't have a measurement necessarily before, but the measurement  
16 afterwards shows that people's trust and their confidence in the service has rebounded as  
17 a result of it they understand that now that we're using more secure protocols to  
18 communicate and to transfer their data.

19 \* \* \*

20 I would just make the observation that protection and trust really come as a function of  
21 security and privacy, but there is a tension between those two.

22 \* \* \*

23 Mayer: ...whether or not they're coming through the official system to get data, they are  
24 in fact getting data and so we can do what we can do in order to protect our users, which  
25 is usually through encryption methods and the like . . . .

26 229. The statements referenced in ¶ 228 above were materially false and/or misleading for the  
27 reasons set forth in ¶ 155 (i)-(v), (vii)-(ix), and (xi) above.

28 230. On March 15, 2015, Yahoo posted on its official website the following statements from  
Alex Stamos:

At Yahoo, we're committed to protecting our users' security. That's why I'm so proud to  
share some updates on our latest security innovation: an end-to-end (e2e) encryption  
extension for Yahoo Mail.



1 Just a few years ago, e2e encryption was not widely discussed, nor widely understood.  
2 Today, our users are much more conscious of the need to stay secure online. There is a  
3 wide spectrum of use for e2e encryption, ranging from the straightforward (sharing tax  
4 forms with an accountant), to the potentially life-threatening (emailing in a country that  
5 does not respect freedom of expression). Wherever you land on the spectrum, we've  
6 heard you loud and clear: We're building the best products to ensure a more secure user  
7 experience and overall digital ecosystem.

8 231. The statements referenced in ¶ 230 above were materially false and/or misleading for the  
9 reasons set forth in ¶ 155 (i)-(v), (vii)-(ix), and (xi) above.

10 232. On or around March 26, 2015, Yahoo made the following representations on its official  
11 website:

12 Our Users First Approach in Action  
13 Protecting Users . . .

14 We've encrypted many of our most important products and services to protect  
15 against snooping by governments or other actors. This includes:

16 Encryption of the traffic moving between Yahoo data centers;

17 Making browsing over HTTPS the default on Yahoo Mail and Yahoo  
18 Homepage;

19 Implementing the latest in security best-practices, including supporting TLS  
20 1.2, Perfect Forward Secrecy and a 2048-bit RSA key for many of our global  
21 properties such as Homepage, Mail, and Digital Magazines; and

22 We've also rolled out an end-to-end (e2e) encryption extension for Yahoo  
23 Mail, now available on GitHub. We are committed to the security of this  
24 solution and oppose mandates to deliberately weaken it or any other  
25 cryptographic system.

26 We are committed to notifying users when we strongly suspect they may  
27 have been the target of a state-sponsored attack.

28 233. The statements referenced in ¶ 232 above were materially false and/or misleading for the  
reasons set forth in ¶ 155 (i)-(v), (vii)-(ix), and (xi) above.

234. On March 26, 2015, Yahoo posted on its official website the following statements from  
Ronald Bell:

At Yahoo, users always come first . . .

As we note in our transparency report, we've encrypted many of our most important  
products and services to protect against unauthorized access by governments or other

1 actors. We recently rolled out an end-to-end (e2e) encryption extension for Yahoo Mail,  
2 now available on GitHub.

3 235. The statements referenced in ¶ 234 above were materially false and/or misleading for the  
4 reasons set forth in ¶ 155 (i)-(v), (vii)-(ix), and (xi) above.

5 236. On May 4, 2015, Yahoo posted on its official website the following statements from  
6 Sean Zadig, Senior Manager, Yahoo E-Crime Investigations, about how Yahoo protects its users from  
7 online criminals:

8 Good governance and Users First: We adhere to the laws of the countries in which we  
9 operate, our Terms of Service, and our Privacy Policy. We encrypt our products . . .

10 237. The statements referenced in ¶ 236 above were materially false and/or misleading for the  
11 reasons set forth in ¶ 155 (i)-(v), (vii)-(ix), and (xi) above.

12 238. On May 7, 2015, Yahoo filed a Quarterly Report on Form 10-Q with the SEC (the “Q1  
13 2015 10-Q”). The Q1 2015 10-Q disclosed the following with respect to risks of data breaches:

14 If our security measures are breached, our products and services may be perceived as not  
15 being secure, users and customers may curtail or stop using our products and services,  
16 and we may incur significant legal and financial exposure.

17 Our products and services involve the storage and transmission of Yahoo’s users’ and  
18 customers’ personal and proprietary information in our facilities and on our equipment,  
19 networks and corporate systems. Security breaches expose us to a risk of loss of this  
20 information, litigation, remediation costs, increased costs for security measures, loss of  
21 revenue, damage to our reputation, and potential liability. Outside parties may attempt to  
22 fraudulently induce employees, users, or customers to disclose sensitive information to  
23 gain access to our data or our users’ or customers’ data. In addition, hardware, software  
24 or applications we procure from third parties may contain defects in design or  
25 manufacture or other problems that could unexpectedly compromise network and data  
26 security. Security breaches or unauthorized access have resulted in and may in the future  
27 result in a combination of significant legal and financial exposure, increased remediation  
28 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.

1           239. The Q1 2015 10-Q contained signed certifications pursuant to SOX by Defendant  
2 Mayer, stating that the financial information contained in the Q1 2015 10-Q was accurate.

3           240. The statements referenced in ¶ 238 above were materially false and/or misleading for the  
4 reasons set forth in ¶ 155 (i)-(v), (vii)-(ix), and (xi) above.

5           241. On July 22, 2015, in a conference call with investors, Defendant Mayer stated that at  
6 Yahoo, “we continue to protect our mail users with new investments in spam and phishing detection.”  
7

8           242. The statements referenced in ¶ 241 above were materially false and/or misleading for the  
9 reasons set forth in ¶ 155 (i)-(v), (vii)-(ix), and (xi) above.

10           243. On August 7, 2015, Yahoo filed a Quarterly Report on Form 10-Q with the SEC (the  
11 “Q2 2015 10-Q”). The Q2 2015 10-Q disclosed the following with respect to risks of data breaches:  
12

13           If our security measures are breached, our products and services may be perceived as not  
14 being secure, users and customers may curtail or stop using our products and services,  
and we may incur significant legal and financial exposure.

15           Our products and services involve the storage and transmission of Yahoo’s users’ and  
16 customers’ personal and proprietary information in our facilities and on our equipment,  
17 networks and corporate systems. Security breaches expose us to a risk of loss of this  
18 information, litigation, remediation costs, increased costs for security measures, loss of  
19 revenue, damage to our reputation, and potential liability. Outside parties may attempt to  
20 fraudulently induce employees, users, or customers to disclose sensitive information to  
21 gain access to our data or our users’ or customers’ data. In addition, hardware, software  
22 or applications we procure from third parties may contain defects in design or  
23 manufacture or other problems that could unexpectedly compromise network and data  
24 security. Security breaches or unauthorized access have resulted in and may in the future  
25 result in a combination of significant legal and financial exposure, increased remediation  
26 and other costs, damage to our reputation and a loss of confidence in the security of our  
27 products, services and networks that could have an adverse effect on our business. We  
28 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.

1           244. The Q2 2015 10-Q contained signed certifications pursuant to SOX by Defendant  
2 Mayer, stating that the financial information contained in the Q2 2015 10-Q was accurate.

3           245. The statements referenced in ¶ 243 above were materially false and/or misleading for the  
4 reasons set forth in ¶ 155 (i)-(v), (vii)-(ix), and (xi) above.

5           246. On September 17, 2015, Yahoo posted on its official website the following statements  
6 from Daryl Low, Tech Yahoo, Architect:

7           At Yahoo, we're committed to protecting our users' security, and we're proud that our  
8 network supports HTTPS across the board . . .

9           Since we first began deploying encryption technologies across our network, we've  
10 worked with thousands of our partners across all of Yahoo's hundreds of global  
11 properties to make sure that any data that is running on our network is secure. This  
12 continues to be an area of focus for us, and we're in a unique position to move the needle  
by encouraging our broad array of partners to move to HTTPS.

13           247. The statements referenced in ¶ 246 above were materially false and/or misleading for the  
14 reasons set forth in ¶ 155 (i)-(v), (vii)-(ix), and (xi) above.

15           248. On October 26, 2015, Yahoo issued a press release praising Yahoo's commitment to  
16 protecting its users' security: "Yahoo! Inc. (NASDAQ:YHOO) announced today that Bob Lord will  
17 join as the Company's Chief Information Security Officer (CISO) . . . Yahoo is committed to protecting  
18 their users' security and maintaining their users' trust. Yahoo offers users encrypted products, provides  
19 an end-to-end encryption plugin on GitHub for Yahoo Mail, offers two-factor authentication, and  
20 recently launched Yahoo Account Key, which allows users a fast and secure way to access their Yahoo  
21 accounts."  
22

23           249. In the same press release, Yahoo represented that " Lord will lead Yahoo's security team  
24 -- known as the Paranoids -- in offensive and defensive protection of the Company's more than one  
25 billion users around the world, and for Yahoo's employees globally. Lord will work closely across all  
26 of the Company's teams and collaboratively within the industry to ensure that Yahoo continues to  
27 provide the highest level of security possible to their users."  
28

1 250. This press release was re-tweeted by Defendant Mayer on the same date.

2 251. The statements referenced in ¶¶ 248-50 above were materially false and/or misleading  
3 for the reasons set forth in ¶ 155 (i)-(v), (vii)-(ix), and (xi) above.

4 252. On November 5, 2015, Yahoo filed a Quarterly Report on Form 10-Q with the SEC (the  
5 “Q3 2015 10-Q”). The Q3 2015 10-Q disclosed the following with respect to risks of data breaches:

6  
7 If our security measures are breached, our products and services may be perceived as not  
8 being secure, users and customers may curtail or stop using our products and services,  
9 and we may incur significant legal and financial exposure.

10 Our products and services involve the storage and transmission of Yahoo’s users’ and  
11 customers’ personal and proprietary information in our facilities and on our equipment,  
12 networks and corporate systems. Security breaches expose us to a risk of loss of this  
13 information, litigation, remediation costs, increased costs for security measures, loss of  
14 revenue, damage to our reputation, and potential liability. Outside parties may attempt to  
15 fraudulently induce employees, users, or customers to disclose sensitive information to  
16 gain access to our data or our users’ or customers’ data. In addition, hardware, software  
17 or applications we procure from third parties may contain defects in design or  
18 manufacture or other problems that could unexpectedly compromise network and data  
19 security. Security breaches or unauthorized access have resulted in and may in the future  
20 result in a combination of significant legal and financial exposure, increased remediation  
21 and other costs, damage to our reputation and a loss of confidence in the security of our  
22 products, services and networks that could have an adverse effect on our business. We  
23 take steps to prevent unauthorized access to our corporate systems, however, because the  
24 techniques used to obtain unauthorized access, disable or degrade service, or sabotage  
25 systems change frequently or may be designed to remain dormant until a triggering  
26 event, we may be unable to anticipate these techniques or implement adequate  
27 preventative measures. If an actual or perceived breach of our security occurs, the  
28 market perception of the effectiveness of our security measures could be harmed and we  
could lose users and customers.

21 253. The Q3 2015 10-Q contained signed certifications pursuant to SOX by Defendant  
22 Mayer, stating that the financial information contained in the Q3 2015 10-Q was accurate.

23 254. The statements referenced in ¶ 252 above were materially false and/or misleading for the  
24 reasons set forth in ¶ 155 (i)-(v), (vii)-(ix), and (xi) above.

25 255. On November 23, 2015, Yahoo made the following public representations as part of its  
26 Privacy Policy, which the Company published on its official website:

1 As always, Yahoo is committed to gaining your trust. Yahoo takes your privacy  
2 seriously . . . We limit access to personal information about you to employees who we  
3 believe reasonably need to come into contact with that information to provide product or  
4 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.

5 256. With respect to Information Sharing and Disclosure, Yahoo’s Privacy Policy made the  
6 following representations:

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

10 We provide the information to trusted partners who work on behalf of or with  
11 Yahoo under confidentiality agreements. These companies may use your  
12 personal information to help Yahoo communicate with you about offers from  
13 Yahoo and our marketing partners. However, these companies do not have any  
14 independent right to share this information.

15 We have a parent's permission to share the information if the user is a child under  
16 age 13. See Children's Privacy & Family Accounts for more information about  
17 our privacy practices for children under 13.

18 We respond to subpoenas, court orders, or legal process (such as law  
19 enforcement requests), or to establish or exercise our legal rights or defend  
20 against legal claims.

21 We believe it is necessary to share information in order to investigate, prevent, or  
22 take action regarding illegal activities, suspected fraud, situations involving  
23 potential threats to the physical safety of any person, violations of Yahoo's terms  
24 of use, or as otherwise required by law.

25 We transfer information about you if Yahoo is acquired by or merged with  
26 another company. In this event, Yahoo will notify you before information about  
27 you is transferred and becomes subject to a different privacy policy.

28 257. Yahoo’s November 2015 Privacy Policy directed visitors to read information under the  
“Security at Yahoo” tab in order “[t]o learn more about security” at the Company. Under that tab,  
Yahoo made the following representations:

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)

1 We use TLS encryption when transmitting certain kinds of information, such as  
2 financial services information or payment information. An icon resembling a  
3 padlock is displayed in most browsers during TLS sessions.

#### 4 Second Sign-in Verification

5 You may turn on a setting that requires a second piece of information such as a  
6 code sent via SMS - in addition to your password - when signing in to your  
7 account from a device or location we don't recognize. (...).

#### 8 On-Demand Passwords

9 Yahoo also offers on-demand passwords. By linking your mobile device to your  
10 account, you enable Yahoo to provide you with an on-demand password sent to  
11 your mobile phone, so you don't have to remember passwords anymore. (...).

#### 12 Secure Storage

13 We deploy industry standard physical, technical, and procedural safeguards that  
14 comply with relevant regulations to protect your personal information.

#### 15 Vendors and Partners

16 To protect the security and privacy of your information, we may provide  
17 information to partners and vendors who work on our behalf or with us under  
18 confidentiality agreements. These companies do not have any independent right  
19 to use or share this information without your consent.

#### 20 Access to Information

21 We limit access to personal information about you to those employees who we  
22 reasonably believe need to come into contact with that information to provide  
23 products or services to you or in order to process this information for us.

#### 24 Education and Training

25 We have implemented a company-wide education and training program about  
26 security that is required of every Yahoo employee.

27 258. The statements referenced in ¶¶ 255-57 above were materially false and/or misleading  
28 for the reasons set forth in ¶ 155 (i)-(v), (vii)-(ix), and (xi) above.

### 29 **D. False and Misleading Statements Made in 2016**

30 259. On February 29, 2016, Yahoo filed an Annual Report on Form 10-K with the SEC (the  
31 "2015 10-K"). The 2015 10-K disclosed the following with respect to risks of data breaches:

32 If our security measures are breached, our products and services may be perceived as not  
33 being secure, users and customers may curtail or stop using our products and services,  
34 and we may incur significant legal and financial exposure.

35 Our products and services involve the storage and transmission of Yahoo's users' and  
36 customers' personal and proprietary information in our facilities and on our equipment,  
37 networks and corporate systems. Security breaches expose us to a risk of loss of this  
38 information, litigation, remediation costs, increased costs for security measures, loss of

1 revenue, damage to our reputation, and potential liability. Outside parties may attempt to  
2 fraudulently induce employees, users, or customers to disclose sensitive information to  
3 gain access to our data or our users' or customers' data. In addition, hardware, software  
4 or applications we procure from third parties may contain defects in design or  
5 manufacture or other problems that could unexpectedly compromise network and data  
6 security. Additionally, some third parties, such as our distribution partners, service  
7 providers and vendors, and app developers, may receive or store information provided  
8 by us or by our users through applications integrated with Yahoo. If these third parties  
9 fail to adopt or adhere to adequate data security practices, or in the event of a breach of  
10 their networks, our data or our users' data may be improperly accessed, used or  
11 disclosed. Security breaches or unauthorized access have resulted in and may in the  
12 future result in a combination of significant legal and financial exposure, increased  
13 remediation and other costs, damage to our reputation and a loss of confidence in the  
14 security of our products, services and networks that could have an adverse effect on our  
15 business. We take steps to prevent unauthorized access to our corporate systems,  
16 however, because the techniques used to obtain unauthorized access, disable or degrade  
17 service, or sabotage systems change frequently or may be designed to remain dormant  
18 until a triggering event, we may be unable to anticipate these techniques or implement  
19 adequate preventative measures. If an actual or perceived breach of our security occurs,  
20 the market perception of the effectiveness of our security measures could be harmed and  
21 we could lose users and customers.

22 260. The 2015 10-K also contained signed certifications pursuant to SOX by Defendant  
23 Mayer, stating that the financial information contained in the 2015 10-K was accurate.

24 261. The statements referenced in ¶ 259 above were materially false and/or misleading for the  
25 reasons set forth in ¶ 155 (i)-(xi) above.

26 262. On March 3, 2016, Yahoo published on its official website statements made by Ron  
27 Bell, observing that “[m]ore than 1 billion users entrust their personal information to Yahoo. [The  
28 company has] built these relationships over more than 20 years in the business,” and stating that “*the  
security of [Yahoo] users’ information is of paramount importance* to them and *to [the] company.*”

29 263. The statements referenced in ¶ 262 above were materially false and/or misleading for the  
30 reasons set forth in ¶ 155 (i)-(xi) above.

31 264. On March 22, 2016, Yahoo posted on its official website the following statements from  
32 Binu Ramakrishnan, Security Engineer for Yahoo Mail:



1 At Yahoo, our users send and receive billions of emails everyday. *We work to make*  
2 *Yahoo Mail* easy to use, personalized, and *secure for our hundreds of millions of users*  
3 *around the world*. In line with our efforts to protect our users' data, our security team  
4 recently conducted a study to measure the deployment quality of SMTP STARTTLS  
5 deployments. We found that while the use of STARTTLS is common and widespread,  
6 the growth has slowed in recent years. Providers with good/valid certificates have better  
7 TLS settings compared to others, and we believe there is an important need to improve  
8 the quality of STARTTLS deployments to protect messages – and therefore, users –  
9 from active network attacks.

10 265. The statements referenced in ¶ 264 above were materially false and/or misleading for the  
11 reasons set forth in ¶ 155 (i)-(xi) above.

12 266. On May 10, 2016, Yahoo filed a Quarterly Report on Form 10-Q with the SEC (the “Q1  
13 2016 10-Q”). The Q1 2016 10-Q disclosed the following with respect to risks of data breaches:

14 If our security measures are breached, our products and services may be perceived as not  
15 being secure, users and customers may curtail or stop using our products and services,  
16 and we may incur significant legal and financial exposure.

17 Our products and services involve the storage and transmission of Yahoo's users' and  
18 customers' personal and proprietary information in our facilities and on our equipment,  
19 networks and corporate systems. Security breaches expose us to a risk of loss of this  
20 information, litigation, remediation costs, increased costs for security measures, loss of  
21 revenue, damage to our reputation, and potential liability. Outside parties may attempt to  
22 fraudulently induce employees, users, or customers to disclose sensitive information to  
23 gain access to our data or our users' or customers' data. In addition, hardware, software  
24 or applications we procure from third parties may contain defects in design or  
25 manufacture or other problems that could unexpectedly compromise network and data  
26 security. Additionally, some third parties, such as our distribution partners, service  
27 providers and vendors, and app developers, may receive or store information provided  
28 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.

1           267. The Q1 2016 10-Q contained signed certifications pursuant to SOX by Defendant  
2 Mayer, stating that the financial information contained in the Q1 2016 10-Q was accurate.

3           268. The statements referenced in ¶ 266 above were materially false and/or misleading for the  
4 reasons set forth in ¶ 155 (i)-(xi) above.

5           269. On July 25, 2016, Yahoo publicly announced that it entered into a purchase agreement  
6 with Verizon. Pursuant to the agreement, Verizon would acquire the operating business of Yahoo for  
7 \$4.8 billion. The announcement of the purchase attached the actual purchase agreement. The purchase  
8 agreement specifically stated that Yahoo is not aware of any data breaches:  
9

10           [A]ny incidents of, or third party claims alleging, (i) Security Breaches, unauthorized  
11 access or unauthorized use of any of Seller's or the Business Subsidiaries' information  
12 technology systems or (ii) loss, theft, unauthorized access or acquisition, modification,  
13 disclosure, corruption, or other misuse of any Personal Data in Seller's or the Business  
14 Subsidiaries' possession, or other confidential data owned by Seller or the Business  
15 Subsidiaries (or provided to Seller or the Business Subsidiaries by their customers) in  
16 Seller's or the Business Subsidiaries' possession, in each case (i) and (ii) that could  
17 reasonably be expected to have a Business Material Adverse Effect. Neither Seller nor  
18 the Business Subsidiaries have notified in writing, or to the Knowledge of Seller, been  
19 required by applicable Law or a Governmental Authority to notify in writing, any Person  
20 of any Security Breach. To the Knowledge of Seller, neither Seller nor the Business  
21 Subsidiaries have received any notice of any claims, investigations (including  
22 investigations by a Governmental Authority), or alleged violations of Laws with respect  
23 to Personal Data possessed by Seller or the Business Subsidiaries, in each case that could  
24 reasonably be expected to have a Business Material Adverse Effect.

25           270. The statements referenced in ¶ 269 above were materially false and/or misleading for the  
26 reasons set forth in ¶ 155 (i)-(xi) above.

27           271. On August 8, 2016, Yahoo filed a Quarterly Report on Form 10-Q with the SEC (the  
28 “Q2 2016 10-Q”). The Q2 2016 10-Q disclosed the following with respect to risks of data breaches:

          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

1 revenue, damage to our reputation, and potential liability. Outside parties may attempt to  
2 fraudulently induce employees, users, or customers to disclose sensitive information to  
3 gain access to our data or our users' or customers' data. In addition, hardware, software  
4 or applications we procure from third parties may contain defects in design or  
5 manufacture or other problems that could unexpectedly compromise network and data  
6 security. Additionally, some third parties, such as our distribution partners, service  
7 providers and vendors, and app developers, may receive or store information provided  
8 by us or by our users through applications integrated with Yahoo. If these third parties  
9 fail to adopt or adhere to adequate data security practices, or in the event of a breach of  
10 their networks, our data or our users' data may be improperly accessed, used or  
11 disclosed. Security breaches or unauthorized access have resulted in and may in the  
12 future result in a combination of significant legal and financial exposure, increased  
13 remediation and other costs, damage to our reputation and a loss of confidence in the  
14 security of our products, services and networks that could have an adverse effect on our  
15 business. We take steps to prevent unauthorized access to our corporate systems,  
16 however, because the techniques used to obtain unauthorized access, disable or degrade  
17 service, or sabotage systems change frequently or may be designed to remain dormant  
18 until a triggering event, we may be unable to anticipate these techniques or implement  
19 adequate preventative measures. If an actual or perceived breach of our security occurs,  
20 the market perception of the effectiveness of our security measures could be harmed and  
21 we could lose users and customers.

22 272. The Q2 2016 10-Q contained signed certifications pursuant to SOX by Defendant  
23 Mayer, stating that the financial information contained in the Q2 2016 10-Q was accurate.

24 273. The statements referenced in ¶ 271 above were materially false and/or misleading for the  
25 reasons set forth in ¶ 155 (i)-(xi) above.

26 274. On August 30, 2016, Yahoo updated its Privacy Policy and made the following public  
27 representations on its official website:

28 As always, Yahoo is committed to gaining your trust . . . Yahoo takes your privacy  
seriously . . .

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.

2725. With respect to Information Sharing and Disclosure, Yahoo's Privacy Policy made the  
following representations:

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

3 We provide the information to trusted partners who work on behalf of or with  
4 Yahoo under confidentiality agreements. These companies may use your  
5 personal information to help Yahoo communicate with you about offers from  
Yahoo and our marketing partners. However, these companies do not have any  
independent right to share this information.

6 We have a parent's permission to share the information if the user is a child under  
7 age 13. See Children's Privacy & Family Accounts for more information about  
our privacy practices for children under 13.

8 We respond to subpoenas, court orders, or legal process (such as law  
9 enforcement requests), or to establish or exercise our legal rights or defend  
against legal claims.

10 We believe it is necessary to share information in order to investigate, prevent, or  
11 take action regarding illegal activities, suspected fraud, situations involving  
12 potential threats to the physical safety of any person, violations of Yahoo's terms  
of use, or as otherwise required by law.

13 We transfer information about you if Yahoo is acquired by or merged with  
14 another company. In this event, Yahoo will notify you before information about  
you is transferred and becomes subject to a different privacy policy.

15 276. Yahoo's August 2016 Privacy Policy directed visitors to read information under the  
16 "Security at Yahoo" tab in order "[t]o learn more about security" at the Company. Under that tab,  
17 Yahoo made the following representations:

18 Protecting our systems and our users' information is paramount to ensuring Yahoo users  
19 enjoy a secure user experience and maintaining our users' trust. We have taken the  
20 following measures to protect your information:

21 Transport Layer Security (TLS)

22 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.

23 Second Sign-in Verification

24 You may turn on a setting that requires a second piece of information such as a code sent  
25 via SMS - in addition to your password - when signing in to your account from a device  
or location we don't recognize. (...)

26 On-Demand Passwords

27 Yahoo also offers on-demand passwords. By linking your mobile device to your  
28 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. (...)

Secure Storage

1 We deploy industry standard physical, technical, and procedural safeguards that comply  
2 with relevant regulations to protect your personal information.

3 Vendors and Partners

4 To protect the security and privacy of your information, we may provide information to  
5 partners and vendors who work on our behalf or with us under confidentiality  
6 agreements. These companies do not have any independent right to use or share this  
7 information without your consent.

8 Access to Information

9 We limit access to personal information about you to those employees who we  
10 reasonably believe need to come into contact with that information to provide products  
11 or services to you or in order to process this information for us.

12 Education and Training

13 We have implemented a company-wide education and training program about security  
14 that is required of every Yahoo employee. (...)

15 Please note that no data transmission over the Internet or information storage technology  
16 can be guaranteed to be 100% secure. We continue to evaluate and implement  
17 enhancements in security technology and practices.

18 277. The statements referenced in ¶¶ 274-76 above were materially false and/or misleading  
19 for the reasons set forth in ¶ 155 (i)-(xi) above.

20 278. On September 9, 2016, Yahoo filed with the SEC a Proxy Statement Pursuant to Section  
21 14(a) of the Securities Exchange Act of 1934, seeking a vote on Yahoo's proposed sale of its operating  
22 business to Verizon. The Proxy Statement attached the Stock Purchase Agreement between Yahoo and  
23 Verizon, which contained the following representations by Yahoo:

24 [T]here have not been any incidents of, or third party claims alleging, (i) Security  
25 Breaches, unauthorized access or unauthorized use of any of Seller's or the Business  
26 Subsidiaries' information technology systems or (ii) loss, theft, unauthorized access or  
27 acquisition, modification, disclosure, corruption, or other misuse of any Personal Data in  
28 Seller's or the Business Subsidiaries' possession, or other confidential data owned by  
Seller or the Business Subsidiaries (or provided to Seller or the Business Subsidiaries by  
their customers) in Seller's or the Business Subsidiaries' possession, in each case (i) and  
(ii) that could reasonably be expected to have a Business Material Adverse Effect.  
Neither Seller nor the Business Subsidiaries have notified in writing, or to the  
Knowledge of Seller, been required by applicable Law or a Governmental Authority to  
notify in writing, any Person of any Security Breach. To the Knowledge of Seller,  
neither Seller nor the Business Subsidiaries have received any notice of any claims,  
investigations (including investigations by a Governmental Authority), or alleged  
violations of Laws with respect to Personal Data possessed by Seller or the Business  
Subsidiaries, in each case that could reasonably be expected to have a Business Material  
Adverse Effect.

1 279. The Stock Purchase Agreement was signed by Defendant Mayer on behalf of Yahoo.

2 280. The statements referenced in ¶ 278 above were materially false and/or misleading for the  
3 reasons set forth in ¶ 155 (iii)-(vi) above.  
4

### 5 **The Truth Begins to Emerge**

6 281. On May 18, 2015, Dow Jones announced that Yahoo's CIO (Chief Information Officer),  
7 Mike Kail, left the Company after less than one year.

8 282. On this news, Yahoo's share price fell \$3.38, or 7.6%, to close at \$40.98 on May 19,  
9 2015, the following trading day.  
10

11 283. On July 28, 2015, Ramses Martinez, Yahoo's interim CISO, posted a report on Yahoo's  
12 Tumblr blogging platform, entitled "Yahoo's Pays \$1M to Network Vulnerability Reporters," providing  
13 some details on Yahoo's "Bug Bounty" program, which Ramses described as "a feedback loop to  
14 determine the effectiveness of our application security controls." Ramses' report stated, in part:

15 Below are some key data points from our Bug Bounty program to date, which we'll  
16 continue to update to help the security community understand the efficacy of this work  
17 and help focus research in this space:

- 18 • To date, we've paid out +\$1M to security vulnerability reporters.
- 19 • Submissions since the inception of the program have now reached the 10,000 mark.
- 20 • Approximately 1,500 of these 10,000 reports have resulted in a bounty payout.
- 21 • The current monthly validity rate of submissions is around 15%, an increase from  
22 10% at the end of 2014.
- 23 • More than 1,800 reporters have participated in the program, about 600 of these have  
24 reported verifiable bugs.
- 25 • 50% of the submissions are from the top 6% set of contributors.
- 26 • 87% of researchers submit less than 10 bugs, this equates to about 34% of all  
27 submissions.

28 284. Following Martinez's posting, Yahoo's share price fell \$0.30, or 0.80% over the  
following two trading days, to close at \$37.42 on July 30, 2015.

1 285. On September 11, 2015, the online publication *TechCrunch* reported that Yahoo's  
2 interim chief information security officer, Ramses Martinez, "quietly left the company in August for a  
3 security role at Apple." *TechCrunch* reported, in relevant part:

4 The news of Martinez departing Yahoo and joining Apple had not been announced but  
5 the details are confirmed in his LinkedIn profile, which notes that he joined Apple in  
6 August of this year as part of the Cupertino company's information security team.

7 Reached for comment, Yahoo says that it is currently looking for a permanent CISO.  
8 "SVP Jay Rossiter is guiding our security team while we continue our search for Yahoo's  
9 next CISO," said a spokesperson for the company.

10 Martinez had only been appointed to the role in July, when the former CISO, Alex  
11 Stamos, was poached by Facebook. He had been with the company since 2011.

12 At a time when cybersecurity has been a[n] increasing issue due to hacking incidents and  
13 developments involving the NSA and snooping by government authorities, Martinez  
14 oversaw a number of security initiatives at Yahoo.

15 They included the company corporate incident response policy, risk analysis process,  
16 threat matrix, and standards; creating and managing the company's global incident  
17 response program; liaising with law enforcement during security incidents and  
18 investigations; and founding and managing the company's bug bounty program.

19 286. On September 14, 2015, New Vision reported a serious security bug in Yahoo  
20 Messenger. "[O]n some Yahoo Messenger emoticon downloads, those cartoon facial expressions are  
21 hiding a serious vulnerability that hackers can exploit. Worse, while cybersecurity experts say they first  
22 alerted Yahoo to the problem last year, Yahoo has reportedly refused to fix it."

23 287. On this news, Yahoo's share price fell \$1.11, or 3.53%, to close at \$30.32 on September  
24 14, 2015, the following trading day.

25 288. On December 2, 2015, the New York Times reported that the Board of Yahoo would  
26 hold a series of meetings to review the possibility of selling its main business. The New York Times  
27 report came after Yahoo shareholder Starboard Value LP urged the Company to drop its plans to hive  
28 off the stake in the Chinese e-commerce company Alibaba and instead to review the possibility of  
selling its core search and display advertising businesses. On the morning of December 3, 2015, Dow  
Jones reported that Alibaba was unlikely to buy Yahoo's core business. Later that day, Bloomberg

1 reported that Yahoo shares had fallen in price after reports that Alibaba was not interested in Yahoo's  
2 core business.

3 289. On this news, Yahoo's share price fell \$1.31, or 3.67%, to close at \$34.34 on December  
4 3, 2015.

5 290. On January 4, 2016, the New York Post reported that activist hedge fund Starboard  
6 Value, which has been pushing for drastic changes at Yahoo, has already informed the Company of its  
7 intent to wage a proxy battle and nominate its own slate to replace the Board. Also, according to the  
8 New York Post's Claire Atkinson, dissident Yahoo investors are pushing to have the Company sell its  
9 Internet business instead of splitting it off into its own company, as perpetually-beleaguered Yahoo  
10 CEO Marissa Mayer intends.

11 291. On this news, Yahoo's share price fell \$1.86, or 5.59%, to close at \$31.40 on January 4,  
12 2016.

13 292. On January 20, 2016, Emirates News Agency disclosed that a stored cross-site scripting  
14 (XSS) vulnerability in Yahoo Mail that affected more than 300 million email accounts globally was  
15 patched earlier this month. The flaw allowed malicious JavaScript code to be embedded in a specially  
16 formatted email message. The code would be automatically evaluated when the message was viewed.  
17 The JavaScript could be used to then compromise the account, change its settings, and forward or send  
18 email without the user's consent. Similarly, CNET News.com reported on that day that a critical flaw in  
19 Yahoo Mail, which might have allowed attackers to hijack accounts, has been fixed. The vulnerability  
20 would have allowed the embedding of malicious JavaScript code in tailored email messages. A victim  
21 would have needed to do nothing else but read the message, which would then execute the code and  
22 give cyber attackers the ability to fully compromise the account, hijack settings, and either forward or  
23 send email to the attacker's server without the victim's knowledge or consent.  
24  
25  
26  
27  
28



1 293. On this news, Yahoo's share price fell \$0.96, or 3.23%, to close at \$28.78 on January 20,  
2 2016.

3 294. On January 23, 2016, The New York Post reported that Verizon made an \$8 billion bid  
4 for Yahoo's core business. On the night of January 27, 2016, Bob Varettoni, director of corporate  
5 communications for Verizon, told CTFN the rumors are false: "The New York Post was wrong. We've  
6 made no offer to acquire Yahoo."

7  
8 295. On this news, Yahoo's share price fell \$0.94, or 3.17%, to close at \$28.75 on January 28,  
9 2016.

10 296. On February 2, 2016, after market close Yahoo announced that for the fourth quarter of  
11 2015, the Company took a \$4.46 billion goodwill impairment charge.

12 297. On this news, Yahoo's share price fell \$1.38, or 4.75%, to close at \$27.68 on February 3,  
13 2016.

14 298. On May 19, 2016, Dow Jones reported after market close that with just a couple of  
15 weeks before the next round of bids was due for the core assets of Yahoo, offers were expected in the  
16 range of \$2 billion -\$3 billion. The bids were expected to be lower than the \$4 billion - \$8 billion range  
17 that had become conventional wisdom over the past couple of months.

18  
19 299. On this news, Yahoo's share price fell \$0.52, or 1.40%, to close at \$36.50 on May 20,  
20 2016.

21 300. On July 24, 2016, Seeking Alpha reported that Verizon was set to pay \$4.8 billion to  
22 acquire Yahoo in a deal that was likely to be announced before the market opened on Monday, July 25.

23 301. On this news, Yahoo's share price fell \$1.06, or 2.69%, to close at \$38.32 on July 25,  
24 2016.  
25  
26  
27  
28

1 302. On the morning of September 22, 2016, investors learned that a massive data breach had  
2 occurred at Yahoo. *Recode* reported that the Company was about to confirm a large-scale theft of  
3 Yahoo user data.<sup>64</sup>

4 Yahoo is poised to confirm a massive data breach of its service, according to several  
5 sources close to the situation. The company was the victim of hacking that has exposed  
6 several hundred million user accounts.

7 While sources were unspecific about the extent of the incursion, since there is the  
8 likelihood of government investigations and legal action related to the breach, they noted  
9 that it is widespread and serious.

10 Earlier this summer, Yahoo said it was investigating a data breach in which hackers  
11 claimed to have access to 200 million user accounts and one was selling them online.  
12 “It’s as bad as that,” said one source. “Worse, really.”

13 At the same time, *Recode* warned of the negative implications of this breach for the sale of Yahoo’s  
14 core business to Verizon, and specifically for the purchase price.

15 The announcement, which is expected to come this week, also has possible larger  
16 implications for the \$4.8 billion sale of Yahoo’s core business — which is at the core of  
17 this hack — to Verizon. The scale of the liability could bring untold headaches to the  
18 new owners. Shareholders are likely to worry that it could lead to an adjustment in the  
19 price of the transaction.

20 *Recode* observed that, although in August Yahoo had said it was “aware of the claim” by a  
21 cybercriminal to have offered for sale the data from 2012 of 200 million users, Yahoo had not  
22 confirmed any data breach or called for password resets. Now, however, Yahoo was expected to  
23 confirm a data breach and might be compelled to call for password resets.

24 At the time, Yahoo said it was “aware of the claim,” but the company declined to say if  
25 it was legitimate and said that it was investigating the information. But it did not issue a  
26 call for a password reset to users. Now, said sources, Yahoo might have to, although it  
27 will be a case of too little, too late.

28 In the afternoon of the same day, Yahoo issued a press release confirming it had been hacked.<sup>65</sup> Yahoo  
admitted that “information associated with at least 500 million user accounts was stolen” from its

---

<sup>64</sup> Kara Swisher, *Yahoo is expected to confirm a massive data breach, impacting hundreds of millions of users*, *Recode*, Sept. 22, 2016, 2:18 am EDT.

<sup>65</sup> *An Important Message to Yahoo Users on Security*, *Business Wire*, Sept. 22, 2016, 2:28 pm ET.

1 network “in late 2014 by what it believes is a state-sponsored actor.” This information “may have  
2 included names, email addresses, telephone numbers, dates of birth, hashed passwords...and, in some  
3 cases, encrypted or unencrypted security questions and answers.” Yahoo also recommended that “users  
4 who haven’t changed their passwords since 2014 do so.”

5 303. Yahoo’s revelations about the breach, described in news reports as “the largest ever  
6 disclosed,” prompted questions from senior government figures and the media about the timing of  
7 Yahoo’s response. On September 22, 2016, *Dow Jones* reported:<sup>66</sup>

8  
9 The Yahoo breach, and the timing of the disclosure, quickly reverberated in Washington.  
10 Sen. Mark Warner, D-Va., said in a statement, “I am perhaps most troubled by news that  
11 this breach occurred in 2014, and yet the public is only learning details of it today.”<sup>67</sup>

12 Following Yahoo’s confirmation of the breach, *Recode* questioned the timeliness of Yahoo’s  
13 disclosures.

14 Why did it take two years to discover and/or disclose the breach? What other breaches  
15 have there been? Who made the decision not to warn users and urge systemwide  
16 password resets? And, of course, why didn’t management make the dire situation more  
17 clear to bidders for Yahoo’s core business, which is the part of the company impacted?<sup>68</sup>

18 304. Analysts repeatedly observed during the Class Period that Yahoo’s stock price was  
19 greatly affected by Alibaba Group Holding Limited (“Alibaba”),<sup>69</sup> the Chinese e-commerce giant which  
20 traded in the U.S., in which Yahoo held a significant stake which was Yahoo’s largest asset.<sup>70</sup> On  
21 September 22, 2016, news also reached the market that two analysts (Stifel and UBS) had increased

22 <sup>66</sup> *Yahoo Says Breach Affected at Least 500 Million Users*, Dow Jones Newswires, Sept. 22, 2016,  
23 2:50 pm ET.

24 <sup>67</sup> *Id.*

25 <sup>68</sup> K. Swisher and K. Wagner, *Yahoo has confirmed a data breach with 500 million accounts stolen, as questions about disclosure to Verizon and users grow*, *Recode*, Sept. 22, 2016, 3:17 pm EDT.

26 <sup>69</sup> See, e.g., SunTrust Robinson Humphrey, *For years, the value of Yahoo stock has been tied to the value of Alibaba*, July 26, 2016; Rosenblatt Securities, *Yahoo!’s stock price has mirrored the moves of Alibaba’s stock, like a tracking stock, over the past year*, Dec. 10, 2015.

27 <sup>70</sup> See e.g., Susquehanna Financial Group, July 26, 2016, *We believe Yahoo’s core business is worth ~\$5 per share based on VZ’s purchase price of ~\$4.8b...\$26 per share for the BABA stake; see also*  
28 *Yahoo! Inc. Form 10-K for the year ended December 31, 2015, filed Feb. 29, 2016, p. 39.*

1 their price targets and made positive comments on Alibaba.<sup>71</sup> On September 22, 2016, Alibaba's share  
2 price closed at \$109.36, up from a closing price of \$106 on September 21, 2016, an increase of \$3.36 or  
3 3.17%.

4 305. On September 22, 2016, Yahoo's share price was pulled in opposite directions by two  
5 categories of new information: (1) the confirmed negative news of theft of data from at least 500  
6 million accounts, and (2) the positive news regarding Yahoo's largest investment, Alibaba. On  
7 September 22, 2016, Yahoo's share price at close was \$44.15, up from a closing price of \$44.14 on  
8 September 21, a change of \$0.01 or 0.02%. But for the partial revelation of the fraud on this date,  
9 Yahoo investors would have seen a greater appreciation in share price with the news on Alibaba.  
10 Instead, Yahoo investors suffered a loss of the appreciation Yahoo shares should have had, and that loss  
11 was caused by the revelations on this date.  
12

13  
14 306. News coverage and analysis of Yahoo's data breach continued after market close on  
15 September 22 and through September 23, 2016. *Agence France Presse* reported Yahoo "was under  
16 pressure Friday to explain how it sustained such a massive breach in 2014, which possibly affected 500  
17 million accounts."<sup>72</sup> Criticism of Yahoo grew, including from international authorities and from data  
18 security experts. *Computer Weekly* reported action by the U.K.'s Information Commissioner.<sup>73</sup>  
19

20 The UK's privacy watchdog, the Information Commissioner's Office (ICO) has  
indicated that it will be investigating the breach to understand the impact on UK citizens.

21 Information Commissioner Elizabeth Denham said the number of people affected by the  
22 breach is "staggering" and demonstrates just how severe the consequences of a security  
23 hack can be.

24 <sup>71</sup> See, e.g.: D. Defotis, *Alibaba Stock: Why Stifel Sees 23% Upside*, Barron's Emerging Markets  
25 Daily, Sept. 22, 2016, 9:30 am ET; J. Lamb, *UBS Bumps Up Price Target on Alibaba Group Holding  
26 Ltd (BABA) in Light of Promising Long-Term Growth Drivers*, Smarter Analyst, Sept. 22, 2016, 3:46  
pm EDT.

27 <sup>72</sup> G. Jackson, L. Benhamou, *Russia? China? Who hacked Yahoo, and why?*, *Agence France Presse*,  
Sept. 23, 2016, 9:27 am ET.

28 <sup>73</sup> W. Ashford, Security Editor, *Yahoo under fire over data breach affecting 500 million users*,  
*Computer Weekly*, Sept. 23, 2016, 10:45 am ET.

1 “The US authorities will be looking to track down the hackers, but it is our job to ask  
2 serious questions of Yahoo on behalf of British citizens and I am doing that.”

3 Experts in data security questioned when Yahoo was aware of the data theft and how the theft could  
4 have gone unreported for so long, as reported by media, including *Computer Weekly*.<sup>74</sup>

5 While Yahoo has confirmed the breach took place in late 2014, it has not made it clear  
6 exactly when it became aware of the breach, said Keatron Evans, senior security  
7 researcher at Blink Digital Security.

8 “If it happened in 2014, and the company has known about it for the past two years, then  
9 why has it taken so long to reveal the extent of the breach?”

10 ....Troy Gill, manager of security research at AppRiver, said ...”I would be interested to  
11 know the findings by Yahoo when they allegedly investigated the 200 million records  
12 that were for sale on the dark web. Were the records confirmed as valid? If so, why did it  
13 take this long to inform users of the breach and why were no forced password resets  
14 issued prior?”

15 ....Michael Lipinski, CISO and chief security strategist at Securonix, said ...“We can’t  
16 keep accepting this level of ignorance as the best we can do”...adding that he does not  
17 believe it took two years to find the breach.

18 “With the Verizon acquisition in process, there is this thing called due diligence that  
19 happens. I firmly believe that this is only now coming to light due to that due diligence. I  
20 believe someone knew about this earlier,” said Lipinski.

21 “Whether there was a cover up or if this breach was not uncovered for two years, this is  
22 a huge failure of the Yahoo team for not being able to identify this much earlier,” he  
23 said.

24 Lipinski said the Yahoo security team appears to be trying to deflect the risk to users by  
25 saying that passwords were hashed using bcrypt.

26 “Ask them how that worked out for Ashley Madison. They used the same salt hash and  
27 the hackers found a work around to the brute force methods of cracking the password,”  
28 he said.

307. On this news, Yahoo’s share price fell from \$44.15 at close on September 22, to \$42.80  
at close on September 23, 2016, a decline of \$1.35 or 3.06%.

308. On October 6, 2016, after market close, Bloomberg reported that Verizon was pushing  
for a discount from the \$4.8 billion price in the 2016 Agreement in light of the recent hacking  
disclosures.

---

<sup>74</sup> *Id.*

1 309. On this news, Yahoo's share price fell \$0.46, or 1.05%, to close at \$43.22 on October 7,  
2 2016.

3 310. On October 13, 2016, Bloomberg reported that Verizon's general counsel said there was  
4 a "reasonable basis" to believe the Yahoo email breach had a material impact on the deal and that it  
5 could allow Verizon to withdraw from the deal.

6 311. On this news, Yahoo's share price fell \$0.74, or 1.75%, to close at \$41.62 on October  
7 13, 2016.

8 312. On October 18, 2016, Bloomberg reported that Yahoo was cut to hold from buy by  
9 Needham analyst Laura Martin, citing concerns that Verizon will walk away or lower the deal price  
10 after Yahoo disclosed details of the 2014 hack. Reportedly, Verizon was still interested in acquiring  
11 Yahoo but the lack of progress in the investigation concerning the 2014 breach was causing misgivings.

12 313. On this news, Yahoo's share price fell \$0.11, or 0.26%, to close at \$41.68 on October  
13 18, 2016.

14 314. On October 20, 2016, CNN Tech reported "Verizon's deal drama with Yahoo is going to  
15 drag on for a long time." According to CNN, Verizon revealed October 20 that its legal team on the day  
16 before, had held their first call with Yahoo to determine the financial impact of Yahoo's massive  
17 security breach on the pending acquisition. Verizon CFO Fran Shammo had stated "[f]rom what I  
18 understand, that's going to be a long process." CFO Shammo further stated "[t]his was an extremely  
19 large breach that received a lot of attention," and "[w]e have to assume it will have a material impact."  
20 CNN also reported that "[t]he lingering caution on Verizon's side comes in stark opposition to Yahoo's  
21 confident rhetoric this week." The Financial Times also reported on that day that Verizon intended to  
22 demand a discount on the \$4.8 billion price tag after Yahoo was subject to a massive cyber attack.

23 315. On this news, Yahoo's share price fell \$0.35, or 0.82%, to close at \$42.38 on October  
24 20, 2016.

1 316. After market close on December 14, 2016, Yahoo revealed a data breach far larger than  
2 any it had disclosed before, affecting “more than one billion user accounts.”<sup>75</sup>

3 Yahoo believes an unauthorized third party, in August 2013, stole data associated with  
4 more than one billion user accounts. The company has not been able to identify the  
5 intrusion associated with this theft. Yahoo believes this incident is likely distinct from  
6 the incident the company disclosed on September 22, 2016.

7 ....Yahoo is notifying potentially affected users and has taken steps to secure their  
8 accounts, including requiring users to change their passwords.

9 On the next trading day, December 15, 2016, Yahoo’s share price reacted quickly to these disclosures.  
10 In the morning, *Bloomberg* reported the resulting decline in price of Yahoo shares, as well as analysts’  
11 comments on the effect the latest news of a security breach would have on the deal to sell Yahoo’s core  
12 business to Verizon.<sup>76</sup>

13 Yahoo! Inc. fell Thursday after disclosing a second major security breach that may have  
14 affected more than 1 billion user accounts, a development that some analysts say may  
15 lead Verizon Communications Inc. to reconsider its bid for the main web businesses.

16 The revelation may drive the market to consider a higher probability of Verizon walking  
17 away or renegotiating the \$4.8 billion deal price, wrote Joseph Stauff, an analyst at  
18 Susquehanna Financial Group, in a note to clients. The shares fell as much as 3.8  
19 percent, to \$39.37, the biggest drop in a month.

20 *Bloomberg* reported Verizon was in fact said to be exploring changes to its deal with Yahoo following  
21 confirmation of this second major breach.<sup>77</sup>

22 Verizon Communications Inc. is exploring a price cut or possible exit from its \$4.83  
23 billion pending acquisition of Yahoo! Inc., after the company reported a second major e-  
24 mail hack affecting as many as 1 billion users, according to a person familiar with the  
25 matter.

26 ....A legal team led by Verizon General Counsel Craig Silliman is assessing the damage  
27 from the breaches and is working toward either killing the deal or renegotiating the  
28 Yahoo purchase at a lower price, the person said.

---

26 <sup>75</sup> *Important Security Information for Yahoo Users*, Business Wire, Dec. 14, 2016, 4:51 pm EST.

27 <sup>76</sup> S. Moritz and B. Womack, *Yahoo Falls After Hack Raises Possibility Verizon May Reconsider*,  
*Bloomberg News*, Dec. 15, 2016, 10:28 am ET.

28 <sup>77</sup> S. Moritz and B. Womack, *Verizon Said to Explore Lower Price or Even Exit From Yahoo Deal*,  
*Bloomberg News*, Dec. 15, 2016, 11:00 am ET.

1 According to *The Financial Times*, in reaction to the biggest data breach ever reported, “Yahoo shares  
2 dropped 5 percent on Thursday amid worries that the latest hacking revelations could scuttle its deal  
3 with Verizon Communications.”<sup>78</sup>

4 California-based Yahoo revealed on Wednesday that information on more than 1bn users  
5 was stolen in 2013, representing by far the biggest ever data breach. It follows  
6 revelations earlier this year in September about an apparently separate hack that took  
place in 2014 and affected 500m users.

7 The news has once again put Verizon’s deal to buy the company in the spotlight, with  
8 Bloomberg News reporting that the US telecommunications company is weighing  
whether to scrap the deal completely.

9 Yahoo’s shares were off by as much as 6.5 per cent following the Bloomberg  
headlines.

10 “(W)e think that Verizon has a fiduciary duty to its shareholders to at least demand a  
11 discount on the acquisition price,” said Richard Windsor, analyst at Edison Investment  
Research.

12 U.S. and international government figures were critical of Yahoo and demanded explanations for this  
13 second and even larger data breach, according to *The Financial Times*.<sup>79</sup>

14 Ms. Mayer is also facing serious questions from regulators on both sides of the  
15 Atlantic concerned about the sophistication of the company’s cyber defences and how  
long it took to detect the intruder.

16 Mark Warner, a US senator, said it was “deeply troubling” that consumers were first  
17 learning of the breach three years after it occurred. He complained that Yahoo had not  
responded to his requests for briefings on the earlier attack.

18 Regulators in the UK and in Ireland, where Yahoo has its European headquarters,  
19 have demanded further details from the company about how their citizens have been  
affected.....

20 “We are urgently examining the facts that have been made available to us,” said  
21 Helen Dixon, data protection commissioner of Ireland, “in order to ascertain the further  
22 investigative questions we need to pose and steps to be taken in order to ultimately  
conclude if European data protection laws have been breached.”

23 317. On this news, Yahoo’s share price dropped from \$40.91 at close on December 14, to  
24 \$38.41 at close on December 15, 2016, a decline of \$2.50 or 6.11%.

26 \_\_\_\_\_  
27 <sup>78</sup> A. Samson, *Yahoo shares slide as concerns swirl about hack’s effect on Verizon deal*, *The*  
*Financial Times*, Dec. 15, 2016, 11:24 am ET.

28 <sup>79</sup> J. Fontanella-Khan and H. Kuchler, *Verizon takeover in doubt after Yahoo reveals second cyber*  
*hack*, *The Financial Times*, Dec. 15, 2016, 8:12 am updated 3:48 pm ET.





1 323. Defendants had a duty to disclose the whole truth to Plaintiffs and investors:

- 2 (a) By choosing to speak on the topics and subjects outlined herein, in the allegedly  
3 false and misleading statements described herein, Defendants had a duty to  
4 familiarize themselves with the subject matter thereof and a correlating duty to  
5 speak accurately and completely about it;
- 6 (b) By choosing to disclose information about these topics and subjects, Defendants  
7 were under a duty to disclose the whole truth;
- 8 (c) In any instance where Defendants made partial disclosures that conveyed false  
9 impressions, they had a duty to disclose the whole truth;
- 10 (d) To the extent that new information later arose that made any of Defendants'  
11 earlier alleged misstatements misleading or untrue, Defendants were obligated to  
12 disclose the whole truth and to correct their prior misstatements.  
13  
14

15 324. Defendants did not disclose truthful, accurate, and complete information. As outlined  
16 herein, they voluntarily disclosed and discussed information concerning Yahoo that, even when viewed  
17 in the best light imaginable to them, disclosed only partial, deceptive information and misleading half-  
18 truths (and in a more realistic light, was utterly false).  
19

20 325. The Individual Defendants' scienter and intent to deceive are further evidenced by the  
21 following facts:

- 22 • Defendants admitted that they had contemporaneous knowledge of the breaches. For example,  
23 on March 1, 2017, Yahoo admitted that "the Company's information security team had  
24 contemporaneous knowledge of the 2014 compromise of user accounts, as well as incidents by  
25 the same attacker involving cookie forging in 2015 and 2016. In late 2014, senior executives  
26 and relevant legal staff were aware that a state-sponsored actor had accessed certain user  
27 accounts by exploiting the Company's account management tool." Concurrently with this  
28

1 admission, Yahoo penalized Defendants Bell and Mayer in connection with the hacking  
2 incidents. For example, Yahoo announced “management changes,” including the Board’s  
3 decision not to award Defendant Mayer a cash bonus for 2016; Mayer’s “offer” to forego any  
4 2017 annual equity awards; and Bell’s resignation as General Counsel and from all other  
5 positions with the Company without pay.

- 6
- 7 • The FBI agents intricately involved in the investigation of the 2014 Data Breach specifically  
8 singled out Defendant Mayer for her ongoing two-year involvement (since 2014) in the  
9 investigation.
- 10 • The FBI, who worked closely with Defendants from the beginning of the 2014 Data Breach,  
11 immediately noticed evidence that the hackers were affiliated with a Russian intelligence  
12 agency. The British intelligence agency was summoned to help the U.S. probe because the  
13 actions of Russia’s hackers were classified as “hostile.”
- 14
- 15 • Yahoo admitted that “as of December 2014, the information security team, which included  
16 Defendant Stamos, understood that the attacker had exfiltrated copies of user database backup  
17 files containing the personal data of Yahoo users . . . ”
- 18
- 19 • Yahoo’s Board of Directors, including Defendant Mayer, regularly received updates from the  
20 Company’s Chief Information Security Officers, including Defendant Stamos, about  
21 cybersecurity updates, during many meetings, including meetings held on April 8, 2014, June  
22 25, 2014, October 16, 2014, June 23, 2015, October 14-15, 2015, and April 13-14, 2016. The  
23 Board, including Defendant Mayer, had knowledge of and received regular updates on the 2014  
24 Data Breach starting at least as early as October 2014 and continuing until at least April 2016.
- 25
- 26 • Confidential witnesses corroborate that Defendants knew of the 2013 and 2014 breaches soon  
27 after they occurred and years before they were publicly disclosed. CW1 stated that Defendant  
28 Mayer received daily updates of the breaches. Yahoo was trying to trouble shoot the hacked

1 email accounts during both the 2013 and 2014 breaches. According to CW1, Mayer did not  
2 want to publicize the breaches.

- 3 • Despite knowing that Yahoo had been a target of nation-state spies, including repeated attacks  
4 by Russian hackers, Defendant Mayer refused to implement even the most rudimentary security  
5 measures, frequently clashing with Defendant Stamos “for fear that even something as simple as  
6 a password change would drive Yahoo’s shrinking email users to other services.”
- 7 • Defendants rejected requests for assistance from third party intelligence officers who  
8 independently identified a group of hackers claiming to have possession of a database of logins  
9 for up to one billion Yahoo accounts, for fear of jeopardizing the Verizon transaction. Yahoo  
10 employed a similar dismissive approach in connection with the 2014 Data Breach, refusing to  
11 confirm a notorious hacker’s claim in July 2016 that he was in possession of account names and  
12 passwords of 200 million Yahoo users. Only after the Verizon deal was sealed did Yahoo  
13 belatedly acknowledge that a state-sponsored hack affected more than 500 million Yahoo  
14 accounts.
- 15 • Despite their concurrent knowledge of the 2013, the 2014, and the Forged Cookies data  
16 breaches, Defendants falsely represented in a September 9, 2016 regulatory filing with the SEC  
17 that “there have not been any incidents of, or third-party claims alleging, (i) Security Breaches,  
18 unauthorized access or unauthorized use of any of Seller’s or the Business Subsidiaries’  
19 information technology systems or (ii) loss, theft, unauthorized access or acquisition,  
20 modification, disclosure, corruption, or other misuse of any Personal Data” in Yahoo’s  
21 possession.

### 22 **PLAINTIFFS’ CLASS ACTION ALLEGATIONS**

23 326. Plaintiffs bring this action as a class action pursuant to Federal Rule of Civil Procedure  
24 23(a) and (b)(3) on behalf of a Class, consisting of all those who purchased or otherwise acquired  
25

1 Yahoo common shares traded on the NASDAQ during the Class Period (the “Class”) and were  
2 damaged upon the revelation of the alleged corrective disclosures. Excluded from the Class are  
3 Defendants herein, the officers and directors of the Company, at all relevant times, members of their  
4 immediate families and their legal representatives, heirs, successors or assigns and any entity in which  
5 Defendants have or had a controlling interest.

6  
7 327. The members of the Class are so numerous that joinder of all members is impracticable.  
8 Throughout the Class Period, Yahoo securities were actively traded on the NASDAQ. While the exact  
9 number of Class members is unknown to Plaintiffs at this time and can be ascertained only through  
10 appropriate discovery, Plaintiffs believe that there are hundreds or thousands of members in the  
11 proposed Class. Record owners and other members of the Class may be identified from records  
12 maintained by Yahoo or its transfer agent and may be notified of the pendency of this action by mail,  
13 using the form of notice similar to that customarily used in securities class actions.  
14

15 328. Plaintiffs’ claims are typical of the claims of the members of the Class as all members of  
16 the Class are similarly affected by Defendants’ wrongful conduct in violation of federal law that is  
17 complained of herein.

18  
19 329. Plaintiffs will fairly and adequately protect the interests of the members of the Class and  
20 have retained counsel competent and experienced in class and securities litigation. Plaintiffs have no  
21 interests antagonistic to or in conflict with those of the Class.

22 330. Common questions of law and fact exist as to all members of the Class and predominate  
23 over any questions solely affecting individual members of the Class. Among the questions of law and  
24 fact common to the Class are:

- 25  
26 • whether the federal securities laws were violated by Defendants’ acts as alleged  
27 herein;  
28 • whether statements made by Defendants to the investing public during the Class  
Period misrepresented material facts about Yahoo’s data safety;

- whether Defendants caused Yahoo to issue false and misleading financial statements during the Class Period;
- whether Defendants acted knowingly or recklessly in issuing false and misleading financial statements;
- whether the prices of Yahoo securities during the Class Period were artificially inflated because of Defendants' conduct complained of herein; and
- whether the members of the Class have sustained damages and, if so, what is the proper measure of damages.

331. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. Furthermore, as the damages suffered by individual Class members may be relatively small, the expense and burden of individual litigation make it impossible for members of the Class to individually redress the wrongs done to them. There will be no difficulty in the management of this action as a class action.

332. Plaintiffs will rely, in part, upon the presumption of reliance established by the fraud-on-the-market doctrine in that:

- Defendants made public misrepresentations or failed to disclose material facts during the Class Period;
- the omissions and misrepresentations were material;
- Yahoo securities are traded in efficient markets;
- the Company's shares were liquid and traded with moderate to heavy volume during the Class Period;
- the Company traded on the NASDAQ, and was covered by multiple analysts;
- the misrepresentations and omissions alleged would tend to induce a reasonable investor to misjudge the value of the Company's common shares; and
- Plaintiffs and members of the Class purchased and/or sold Yahoo common shares between the time the Defendants failed to disclose or misrepresented material facts and the time the true facts were disclosed, without knowledge of the omitted or misrepresented facts.

333. Based upon the foregoing, Plaintiffs and the members of the Class are entitled to a presumption of reliance upon the integrity of the market.

1 334. Alternatively, Plaintiffs and the members of the Class are entitled to the presumption of  
2 reliance established by the Supreme Court in *Affiliated Ute Citizens of the State of Utah v. United*  
3 *States*, 406 U.S. 128, 92 S. Ct. 2430 (1972), as Defendants omitted material information in their Class  
4 Period statements in violation of a duty to disclose such information.

5 **COUNT I**

6 **Violation of Section 10(b) of the Exchange Act and Rule 10b-5**  
7 **Against All Defendants**

8 335. Plaintiffs repeat and reallege each and every allegation contained above as if fully set  
9 forth herein.

10 336. This Count is asserted against Yahoo and the Individual Defendants and is based upon  
11 Section 10(b) of the Exchange Act, 15 U.S.C. § 78j(b), and Rule 10b-5 promulgated thereunder by the  
12 SEC.

13 337. During the Class Period, Yahoo and the Individual Defendants, individually and in  
14 concert, directly or indirectly, disseminated or approved the false statements specified above, which  
15 they knew or deliberately disregarded were misleading in that they contained misrepresentations and  
16 failed to disclose material facts necessary in order to make the statements made, in light of the  
17 circumstances under which they were made, not misleading.

18 338. Yahoo and the Individual Defendants violated §10(b) of the 1934 Act and Rule 10b-5 in  
19 that they:

- 20 • employed devices, schemes and artifices to defraud;
- 21 • made untrue statements of material facts or omitted to state material facts  
22 necessary in order to make the statements made, in light of the circumstances  
23 under which they were made, not misleading; or
- 24 • engaged in acts, practices and a course of business that operated as a fraud or  
25 deceit upon Plaintiffs and others similarly situated in connection with their  
26 purchases of Yahoo common shares during the Class Period.
- 27
- 28

1 339. Yahoo and the Individual Defendants acted with scienter in that they knew the public  
2 documents and statements issued or disseminated in the name of Yahoo were materially false and  
3 misleading; knew that such statements or documents would be issued or disseminated to the investing  
4 public; and knowingly and substantially participated, or acquiesced in the issuance or dissemination of  
5 such statements or documents as primary violations of the securities laws. These Defendants, by virtue  
6 of their receipt of information reflecting the true facts of Yahoo, their control over, and/or receipt  
7 and/or modification of Yahoo's allegedly materially misleading statements, and/or their associations  
8 with the Company which made them privy to confidential proprietary information concerning Yahoo,  
9 participated in the fraudulent scheme alleged herein.  
10

11 340. The Individual Defendants, who are the senior officers and/or directors of the Company,  
12 had actual knowledge of the material omissions and/or the falsity of the material statements set forth  
13 above, and intended to deceive Plaintiffs and the other members of the Class or, in the alternative, acted  
14 with reckless disregard for the truth when they failed to ascertain and disclose the true facts in the  
15 statements made by them or other Yahoo personnel to members of the investing public, including  
16 Plaintiffs and the Class.  
17

18 341. As a result of the foregoing, the market price of Yahoo common shares was artificially  
19 inflated during the Class Period. In ignorance of the falsity of Yahoo's and the Individual Defendants'  
20 statements, Plaintiffs and the other members of the Class relied on the statements described above  
21 and/or the integrity of the market price of Yahoo common shares during the Class Period in purchasing  
22 Yahoo common shares at prices that were artificially inflated as a result of Yahoo's and the Individual  
23 Defendants' false and misleading statements.  
24

25 342. Had Plaintiffs and the other members of the Class been aware that the market price of  
26 Yahoo securities had been artificially and falsely inflated by Yahoo and the Individual Defendants'  
27 misleading statements and by the material adverse information which Yahoo and the Individual  
28



1 Defendants did not disclose, they would not have purchased Yahoo's common shares at the artificially  
2 inflated prices that they did, or at all.

3 343. As a result of the wrongful conduct alleged herein, Plaintiffs and other members of the  
4 Class have suffered damages in an amount to be established at trial.

5 344. By reason of the foregoing, Yahoo and the Individual Defendants have violated Section  
6 10(b) of the 1934 Act and Rule 10b-5 promulgated thereunder and are liable to the Plaintiffs and the  
7 other members of the Class for substantial damages which they suffered in connection with their  
8 purchase of Yahoo common shares during the Class Period.  
9

10 **COUNT II**

11 **Violation of Section 20(a) of the Exchange Act**  
12 **Against The Individual Defendants**

13 345. Plaintiffs repeat and reallege each and every allegation contained in the foregoing  
14 paragraphs as if fully set forth herein.

15 346. During the Class Period, the Individual Defendants participated in the operation and  
16 management of Yahoo, and conducted and participated, directly and indirectly, in the conduct of  
17 Yahoo's operations, including its security protocols. Because of their senior positions, they knew of the  
18 adverse non-public information regarding the Company's inadequate internal safeguards in data  
19 security protocols.  
20

21 347. As officers and/or directors of a publicly owned company, the Individual Defendants had  
22 a duty to disseminate accurate and truthful information with respect to Yahoo's data safety and  
23 operations, and to correct promptly any public statements issued by Yahoo which had become  
24 materially false or misleading.  
25

26 348. Because of their positions of control and authority as senior officers, the Individual  
27 Defendants were able to, and did, control the contents of the various reports, statements, press releases  
28 and public filings which Yahoo disseminated in the marketplace during the Class Period. Throughout

1 the Class Period, the Individual Defendants exercised their power and authority to cause Yahoo to  
2 engage in the wrongful acts complained of herein. The Individual Defendants, therefore, were  
3 “controlling persons” of Yahoo within the meaning of Section 20(a) of the Exchange Act. In this  
4 capacity, they participated in the unlawful conduct alleged, which artificially inflated the market price  
5 of Yahoo common shares.

6  
7 349. By reason of the above conduct, the Individual Defendants are liable pursuant to Section  
8 20(a) of the Exchange Act for the violations committed by Yahoo.

9 **PRAYER FOR RELIEF**

10 WHEREFORE, Plaintiffs demand judgment against Defendants as follows:

11 A. Determining that the instant action may be maintained as a class action under Rule 23 of  
12 the Federal Rules of Civil Procedure, and certifying Plaintiffs as the Class representatives;

13  
14 B. Requiring Defendants to pay damages sustained by Plaintiffs and the Class by reason of  
15 the acts and transactions alleged herein;

16 C. Awarding Plaintiffs and the other members of the Class pre-judgment and post-judgment  
17 interest, as well as their reasonable attorneys’ fees, expert fees and other costs; and

18 D. Awarding such other and further relief as this Court may deem just and proper.  
19

20  
21 **DEMAND FOR TRIAL BY JURY**

22 Plaintiffs hereby demand a trial by jury.

23 Dated: June 7, 2017

24 Respectfully submitted,

25 **POMERANTZ LLP**

26 By: /s/ Jeremy A. Lieberman  
27 Jeremy A. Lieberman  
28 Emma Gilmore  
600 Third Avenue, 20th Floor  
New York, New York 10016

1 Telephone: (212) 661-1100  
2 Facsimile: (212) 661-8665  
3 Email: [jalieberman@pomlaw.com](mailto:jalieberman@pomlaw.com)  
4 Email: [egilmore@pomlaw.com](mailto:egilmore@pomlaw.com)

5 **POMERANTZ LLP**  
6 Patrick V. Dahlstrom  
7 Ten South La Salle Street, Suite 3505  
8 Chicago, Illinois 60603  
9 Telephone: (312) 377-1181  
10 Facsimile: (312) 377-1184  
11 Email: [pdahlstrom@pomlaw.com](mailto:pdahlstrom@pomlaw.com)

12 **GLANCY PRONGAY & MURRAY LLP**  
13 Joshua L. Crowell  
14 Jennifer Leinbach  
15 1925 Century Park East, Suite 2100  
16 Los Angeles, California 90067  
17 Telephone: (310) 201-9150  
18 Facsimile: (310) 201-9160  
19 E-mail: [jcrowell@glancylaw.com](mailto:jcrowell@glancylaw.com)

20 *Lead counsel*

21 **BRONSTEIN, GEWIRTZ**  
22 **& GROSSMAN, LLC**  
23 Peretz Bronstein  
24 60 East 42nd Street, Suite 4600  
25 New York, NY 10165  
26 Telephone: (212) 697-6484  
27 Facsimile (212) 697-7296  
28 Email: [peretz@bgandg.com](mailto:peretz@bgandg.com)

*Additional counsel*

