



**IN THE COURT OF CHANCERY OF THE STATE OF DELAWARE**

OKLAHOMA FIREFIGHTERS  
PENSION AND RETIREMENT  
SYSTEM, derivatively on behalf of  
YAHOO! INC.,

Plaintiff,

v.

ERIC BRANDT, DAVID FILO,  
CATHERINE FRIEDMAN, MARISSA  
MAYER, THOMAS MCINERNEY,  
JANE E. SHAW, and MAYNARD  
WEBB, JR.

Defendants,

- and -

YAHOO INC., a Delaware corporation,

Nominal Defendant.

PUBLIC VERSION

FILED ON: February 23, 2017

C.A. No. 2017-0133-SG

**VERIFIED DERIVATIVE COMPLAINT**

Plaintiff Oklahoma Firefighters Pension and Retirement System (“Plaintiff”), by and through its undersigned attorneys, brings this action for the benefit of Nominal Defendant Yahoo! Inc. (“Yahoo” or the “Company”).

The allegations in this Verified Shareholder Derivative Complaint are made upon Plaintiff’s personal knowledge with regard to its own acts, and upon

information and belief as to all other matters. Plaintiff's information and belief is based upon, among other things, the investigation conducted by Plaintiff's counsel, Bernstein Litowitz Berger & Grossmann LLP and Friedlander & Gorris, P.A., which included, among other things, review of: (a) documents produced in response to a demand for corporate books and records pursuant to Section 220 of the Delaware General Corporation Law; (b) investigations conducted by the United States Securities and Exchange Commission ("SEC"), the Federal Trade Commission ("FTC"), the Department of Justice ("DOJ"), and other governmental agencies concerning the facts alleged herein; (c) the Company's public filings with the SEC, (d) news articles, conference call transcripts, analysts' reports, and press releases; and (e) other publicly available information pertaining to Yahoo and/or the topics addressed herein.

## **NATURE OF THE ACTION**

1. This stockholder derivative action proves, yet again, that the cover up is almost always worse than the crime.

2. Yahoo is one of the world's leading providers of email and internet services. As part of its core email business, Yahoo stores extensive personal information provided by its hundreds of millions of users.

3. While Yahoo has built a massive user-base, it also has long-faced serious competition. Since providing email and web services is a replaceable commodity, the heart of Yahoo's ability to survive and compete rests on customers' willingness to place their trust in Yahoo.

4. The Board recognizes the importance of maintaining the security of customer information. Indeed, while some boards of directors leave technical jobs like fighting cyberattacks and preserving customer information to management, the Yahoo board of directors (the "Board") has for many years actively and closely monitored the Company's effort to insure the protection of its user data.

5. Even the most sophisticated cyber defense is susceptible to yet more sophisticated hackers. Yahoo has long publicly reported that one of the principal risks in operating an internet conglomerate is that of cybersecurity intrusions.

6. In fact, as Yahoo highlights in its securities filings, almost every state in the country has passed statutes setting comparable standards of care concerning the protection of user data and personal information. These statutes universally make it illegal for any company to improperly delay informing customers of an identified hack of customer data and personal information. Moreover, a company's decision to knowingly, deliberately, or willfully conceal an outside hack of customer information typically provides for treble or punitive damages.

7. Given the importance of protecting user data, the Board knows, and has in its prior response to hacking incidents demonstrated its recognition, of the critical importance of informing users immediately after learning that outside parties have compromised Yahoo's networks and stolen customer information.

8. Yahoo has in the past suffered some outside intrusions that compromised its customer data. The Board was promptly informed about those hacks, how the outside parties broke through Yahoo's cybersecurity measures, what Yahoo's internal cybersecurity department did to fix the problem, and most importantly, exactly how Yahoo informed the affected customers about the theft of their information.

9. This case arises because the Board abandoned its prior course of dealing and compliance with user data laws following a September 2014 intrusion

emanating from [REDACTED] which represented the single largest website hack in history.

10. Yahoo promptly learned of what was internally codenamed [REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

11. Yahoo did not inform the affected customers.

12. While Yahoo has inexplicably withheld or did not maintain minutes for numerous meetings at which the [REDACTED] Intrusion was likely discussed, [REDACTED]

[REDACTED]

[REDACTED]

13. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] (See Ex. 1 attached hereto.) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

14. [REDACTED]

Yahoo's Board did not inform the affected customers.

15. [REDACTED]

[REDACTED]

[REDACTED] Under the circumstances, it is hard to fathom discussions concerning cybersecurity that did not include the [REDACTED] Intrusion.

16. [REDACTED] Yahoo's Board did not inform the affected customers.

17. [REDACTED] amidst efforts to sell Yahoo's web businesses to alleviate the massive pressure building to oust Yahoo Chief Executive Officer Marissa Mayer, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED] [REDACTED]

[REDACTED]

18. [REDACTED] Yahoo's Board did not inform the affected customers.

19. In July 2016, Yahoo agreed to sell its web business to Verizon (the "Verizon Transaction"). Shortly thereafter, as part of Verizon's standard tracking of what is called the "dark web," it identified references to a massive hack of Yahoo's servers.

20. When Verizon asked Yahoo about these rumors, the Board knew it could no longer conceal what had happened. A few weeks later, about two years after the hack took place and at least [REDACTED] after the Board actually knew about the [REDACTED] Intrusion, Yahoo finally disclosed to the public (and to its customers) the hack.

21. Since then, dozens of lawsuits, many seeking treble and/or punitive damages, have been filed. Verizon has delayed the acquisition of Yahoo assets, and is renegotiating the deal terms to account for the consequences of the hack itself, and surely the increased harm resulting from the Board's silence about it.

22. When all is said and done, the Board's knowing concealment of the [REDACTED] Intrusion proves the old maxim: the cover up really is always worse than the crime. Had the Board disclosed the truth from the outset, customers would have been upset, but they would know Yahoo put their interests first. Bidders like Verizon account for the economic effect of the [REDACTED] Intrusion, but the damage to Yahoo's brand and good will in the marketplace would be contained.

23. Instead, customers are not only suing, but the Yahoo brand is irreparably tarnished. Verizon has been gifted significant leverage to extract greater concessions because of that damage to the Yahoo name.

24. As explained herein, Plaintiff seeks to hold the Yahoo Board accountable for its breaches of fiduciary duty.



## **PARTIES**

25. Plaintiff Oklahoma Firefighters Pension and Retirement System (“Plaintiff”) is a retirement system based in Oklahoma City, Oklahoma, providing retirement allowances and other benefits to firefighters in Oklahoma. Plaintiff has owned and continues to own Yahoo shares continuously at all relevant times alleged herein. Plaintiff will retain shares of Yahoo through the course of this litigation.

26. Nominal Defendant Yahoo is a Delaware corporation, with its principal place of business located in Palo Alto, California. Yahoo’s shares trade on the NASDAQ Stock Market under ticker symbol “YHOO.” Yahoo, along with its subsidiaries, incorporated in 1995, is engaged in digital information discovery. The Company focuses on informing, connecting and entertaining its users with its search (Yahoo Search), communications (Yahoo Mail and Yahoo Messenger), and digital content products, such as Yahoo News, Yahoo Sports, Yahoo Finance and Yahoo Lifestyle. As part of its core business, Yahoo collects, stores, and mines user data for profit.

27. Defendant Eric Brandt has served as Chairman of the Board since January 2017 and a director since March 2016. Defendant Brandt has served as the Chairman of the Audit and Finance Committee since March 2016.

28. Defendant David Filo is a founder of the Company, has served as an officer of Yahoo since March 1995, and as a director since June 2014.

29. Defendant Catherine Friedman has served as a director since March 2016.

30. Defendant Marissa Mayer has served as Chief Executive Officer, President, and a director since July 2012. Defendant Mayer was a regular attendee at Audit and Finance Committee meetings.

31. Defendant Thomas McInerney has served as a director since April 2012. Defendant McInerney has served as a member of the Audit and Finance Committee since at least January 2014.

32. Defendant Jane E. Shaw has served as a director since June 2014.

33. Defendant Maynard Webb, Jr. currently serves as Chairman Emeritus of the Board. He has been a director since February 2012, and served as interim Chairman of the Board from April 2013 to August 2013 and as Chairman of the Board from August 2013 to January 2017. Defendant Webb was a regular attendee at Audit and Finance Committee meetings.

## **SUBSTANTIVE ALLEGATIONS**

### **I. YAHOO'S BUSINESS DEPENDS ON CUSTOMER TRUST**

34. Yahoo is a leading Internet company that provides Internet-based services to hundreds of millions of users. As part of its internet business, Yahoo collects and stores large volumes of sensitive personal information about its users, including users' names, email addresses, telephone numbers, birthdates, passwords, security questions linked to users' accounts, and, of course, users' emails themselves.

35. As detailed below, Yahoo's Board has long-recognized that a failure by the Company to sufficiently protect its customers' information could be devastating to its business, and that the trust that customers place in Yahoo could disappear if the Company failed to timely disclose and contain a theft of user data.

36. According to the Company's most recent Form 10-K, filed on February 29, 2016, the Company recognizes that "[i]f 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."

37. In order to earn and maintain the trust of its hundreds of millions of customers, Yahoo guarantees its users that it will take certain specific steps to

protect their private and personal information. Specifically, Yahoo promises its users on its website and in its Privacy Policy that Yahoo will (i) “take[] your privacy seriously;” (ii) “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 in order to do their jobs;” and (iii) “have physical, electronic, and procedural safeguards that comply with federal regulations to protect personal information about you.”

38. Yahoo’s Board and senior executives understand that securing the personal information of users and customers is critical to the Company’s financial well-being. In its Form 10-K, filed on February 29, 2016, and signed by all then-current members of the Board, the Company repeatedly acknowledges the potential for harm resulting from data breaches: (i) “Security breaches expose us to risk of loss of [users’ and customers’ personal and proprietary] information, litigation, remediation costs, increased costs for security measures, loss of revenue, damage to our reputation, and potential liability;” (ii) “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;” and (iii) “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.”

39. Given the gravity of harm to users and customers resulting from security breaches, forty-seven states, the District of Columbia, Puerto Rico, Guam, and the Virgin Islands have all enacted Unfair, Deceptive or Abusive Acts and Practice (“UDAAP”) and similar consumer protection laws that impose affirmative obligations on companies to timely inform customers in the event of a security breach in order to provide those customers with an opportunity to mitigate any harm resulting from the intrusion. This is especially true where, as here, the company has made affirmative promises to do so in agreements with consumers. Because Yahoo operates in every single one of these states and territories, the Board is well aware of the obligations imposed by these UDAAP and similar consumer protection laws, as well as the adverse consequences the Company would face if it failed to comply with them.

40. Indeed, the Company’s Form 10-K, signed by a majority of the Board, states that “[m]any states have passed laws requiring notification to users where there is a security breach for personal data, such as California’s Information Practices Act.” State consumer protection, data security, and reporting laws

impose damages on companies for failing to notify users of a security breach. Statutory damages for violations of these state law provisions are significant – at least \$1,000 per violation. If a court determines that the failure to notify was willful and deliberate, many of these statutes permit a court to award plaintiffs punitive or treble damages.

41. Consequently, as the Board well understood, failure to take affirmative steps to inform users or customers of a security breach, and particularly, active concealment of a security breach, will very likely result in significant legal liability, erosion of user trust, and resulting harm to the Company's good will and reputation.

## **II. YAHOO'S BOARD WAS REGULARLY BRIEFED ABOUT EVEN MODEST HACKING INCIDENTS AND ACTED TO PRESERVE CUSTOMER TRUST**

42. Given the importance to Yahoo's financial well-being of cybersecurity and compliance with applicable laws and regulations governing user privacy, at almost all meetings, from at least 2014 to the present, the Board or its Audit and Finance Committee received detailed and comprehensive updates about the Company's cybersecurity, including information about weaknesses in and intrusions of Yahoo's data systems.

43. Either the Board or the Audit and Finance Committee received consistent updates on a quarterly basis from the Company’s Chief Information Security Officer (“CISO”).

44. CISO updates typically reviewed recent data security breaches and threats, both large and small. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] (See Ex. 2, at YHOO S’holder Demand 001136.)

45. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

46. The CISO updates also [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

47. The Audit and Finance Committee received CISO or other cybersecurity updates at a minimum of eight meetings, including those held on June 24, 2014, October 15, 2014, April 15, 2015, June 23, 2015, October 14, 2015, December 2, 2015, February 22, 2016, and April 3, 2016.

48. Moreover, the Board received CISO or other cybersecurity updates during at least six meetings, including those held on April 8, 2014, June 25, 2014, October 16, 2014, June 23, 2015, October 14-15, 2015, and April 13-14, 2016.

49. Yahoo's Board and senior management also has an established course of dealing of immediately notifying victims of a security breach. For instance, in July 2012, more than 450,000 Yahoo user accounts were compromised. The Company immediately issued a press release acknowledging the hack and notifying affected users.

50. Less than two years later, in January 2014, Yahoo announced another security breach, but Yahoo did not disclose how many accounts were affected.



Again, Yahoo responded by publicly disclosing the hack and contacting affected users.<sup>1</sup>

51. Given the statements the Board approved in the Company's Form 10-Ks, as well as its experience with prior cybersecurity threats, the Board is aware of its affirmative duty to timely inform users and customers of data breaches.

### **III. THE BOARD RECEIVES REPEATED UPDATES REGARDING THE NOVEMBER 2014 [REDACTED] INTRUSION**

52. Beginning in September 2014, sensitive personal account information associated with at least 500 million user accounts was stolen from the Company's network by a state-sponsored actor. This catastrophic hacking incident, internally labelled as the "[REDACTED] Intrusion," represents *the largest data breach for a single website in history*.

53. The stolen information included users' names, email addresses, telephone numbers, dates of birth, hashed passwords, and, in some cases, encrypted or unencrypted security questions and answers. As a January 2017 article in *The Hill* explained, given the nature of the information stolen, "any sensitive data or documents contained in Yahoo emails could be compromised – not just credit card numbers but bank account numbers, Social Security numbers,

---

<sup>1</sup> "Yahoo Mail Accounts Hacked Through Third-Party," *The Atlantic* (Jan. 30, 2014), *available at*: [www.theatlantic.com/technology/archive/2014/01/yahoo-mail-accounts-hacked-hacked-through-third-party/357558/](http://www.theatlantic.com/technology/archive/2014/01/yahoo-mail-accounts-hacked-hacked-through-third-party/357558/)

driver’s license numbers, passport information, birth certificates, deeds, mortgages and contracts to name just a few.”

54.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] (Ex. 3, at YHOO

S’holder Demand 001297.) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(Ex. 4, at YHOO S’holder Demand 001370.)

55. The scope and nature of the [REDACTED] Intrusion was so troubling that [REDACTED]

56. [REDACTED]

[REDACTED] attached hereto as Ex. 5). [REDACTED]

[REDACTED] (Ex. 5,

at YHOO S'holder Demand 003673.) [REDACTED]

57. [REDACTED]

[REDACTED] (*Id.*) [REDACTED]

[REDACTED] (*Id.* at YHOO S’holder Demand 003670.)

58. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] (Ex. 6, at YHOO S’holder Demand 001774.) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] (Ex. 7, at YHOO S’holder Demand 001805.)

59. [REDACTED]

[REDACTED]

[REDACTED] (Ex. 8, at YHOO S’holder Demand 002082.). [REDACTED]

[REDACTED] (*Id.* at YHOO S’holder Demand 002088.) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] (Ex. 1, at YHOO S’holder Demand 002235-36.) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] (See Ex. 5, at YHOO S’holder Demand 003670.)

60. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Indeed, as discussed above, the Audit and Finance Committee was routinely briefed on security intrusions of all sizes. [REDACTED]

[REDACTED]

[REDACTED]

61. [REDACTED]

[REDACTED] (Ex. 9, at YHOO S’holder Demand 002242.) [REDACTED]

[REDACTED]

[REDACTED] (*Id.* at YHOO S’holder Demand 002252-53.) [REDACTED]

[REDACTED]

---

<sup>2</sup> [REDACTED]

[REDACTED]

[REDACTED] According to the Audit and Finance Committee charter, “[t]he Committee shall regularly report to the Board on Committee findings, recommendations, or other matters the Committee deems appropriate or the Board requests. In connection therewith, the Committee should review with the Board any issues that arise with respect to . . . the Company’s compliance with legal or regulatory requirements[.]” (Ex. 10.)

62. Yahoo’s Corporate Governance Guidelines further provide that the Board is “responsible for overseeing major risks facing the Company as well as the Company’s program to prevent and detect violations of law, regulation, and Company policies and procedures.” (Ex. 11.) [REDACTED]

[REDACTED]

[REDACTED]

63. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] (Ex. 12, at YHOO S’holder Demand 004319.)

64. [REDACTED]

[REDACTED]

[REDACTED] (Ex. 13, at YHOO S'holder Demand 003182.) [REDACTED]

65. [REDACTED]

[REDACTED] (*Id.*) [REDACTED]

[REDACTED]” (*Id.* at 3185.)

66. Again, because the [REDACTED] Intrusion represented the single most significant intrusion in the Company's history, the Board continuously received updates on the Company's handling of the fallout from this hacking incident.

#### **IV. THE BOARD DOES NOT NOTIFY YAHOO USERS OF THE [REDACTED] INTRUSION**

67. As stated above, under consumer fraud and data reporting statutes, a court is permitted to award treble or punitive damages in the event of a willful or knowing violation of the law.

68. Inexplicably, the Board declined to disclose the [REDACTED] Intrusion to Yahoo's affected users for nearly two years.

69. The Board's failure to disclose the existence of “a large-scale intrusion” into Yahoo's internal systems that gave intruders continuous access to

personal user information has exposed the Company to significantly greater liability. In fact, recent class actions filed by users against Yahoo seek recovery of treble and/or punitive damages. Thus, the Board's actions in concealing the [REDACTED] Intrusion have resulted in significantly greater harm to the Company than the hack itself. As discussed in Section VIII, because Verizon will assume an undisclosed portion of the legal liability upon completion of the Verizon Transaction, any adverse adjustment to the terms is, at least in part, a result of the Board's breaches of fiduciary duty.

**V. YAHOO FACES INTENSE PRESSURE TO SELL THE COMPANY'S OPERATING BUSINESS**

70. As noted in a July 2016 *New York Times* article, under Mayer's leadership, Yahoo's core operating business had become a "flailing brand." Yahoo therefore faced intense pressure to sell the operating business.

71. Mayer, in particular, faced enormous pressure to sell Yahoo's operating business because despite being lavishly compensated, she had utterly failed to improve that business's fortunes.

72. When Mayer joined Yahoo as Chief Executive Officer in July 2012, the Company gave Mayer a \$30 million signing bonus and \$14 million to make whole the Google bonuses she was foregoing at the time. With her high pay came soaring expectations to turn around the struggling company.



73. But Mayer failed at virtually every turn. Less than a year into her stint as CEO, Mayer came under repeated attack for failing to turn around Yahoo's business. As early as March 2013, the market had concluded that Mayer was not equipped to run or oversee Yahoo's position. For instance, a March 1, 2013 Forbes article blamed "the lack of strategy, innovation and growth at Yahoo" squarely on "leadership."

74. Mayer's tenure was plagued with high-profile executive departures. Most notably, she oversaw the disastrous hire of former Google employee Henrique De Castro, who received \$108 million for 15 months of work.

75. Mayer also caused the Company to spend billions of dollars on underperforming acquisitions. For instance, in 2014, Yahoo agreed to pay \$1.1 billion to purchase Tumblr to revitalize the Company by co-opting a web property with strong visitor traffic but little revenue. This extravagant bet never panned out, and Tumblr never became a viable social media competitor. Since the acquisition, Yahoo has written down half of Tumblr's acquisition price.

76. By 2015, repeated criticism turned into calls for Mayer's resignation. On October 21, 2015, The Street published an opinion piece entitled, "Why Yahoo CEO Marissa Mayer Must Go." The Street stated its conclusion

bluntly: “After 40 months of ineffectual leadership, it’s time for Yahoo . . . CEO Marissa Mayer to go.”

77. Struggling to achieve any return on investment, public stockholders began to pressure Mayer and the Board to sell Yahoo’s core business, and in February 2016, they finally succumbed to that pressure. In a February 2, 2016 press release, Mayer announced the Company would initiate a bidding process for its core business.

78. Finally, on July 25, 2016, Yahoo announced that Verizon had emerged victorious from the bidding process and would purchase Yahoo’s core operating business for \$4.8 billion. Yahoo billed the asset sale as a significant victory for the Company. In a press release, Mayer stated, “The sale of our operating business, which effectively separates our Asian asset equity stakes, is an important step in our plan to unlock shareholder value for Yahoo. This transaction also sets up a great opportunity for Yahoo to build further distribution and accelerate our work in mobile, video, native advertising and social.”

**VI. THE YAHOO BOARD CONCEALS THE [REDACTED] INTRUSION IN CONNECTION WITH THE VERIZON TRANSACTION.**

79. Under intense pressure from stockholders, and desperate to consummate the Verizon Transaction, the Board made affirmative misrepresentations to Verizon that concealed the [REDACTED] Intrusion.

80. As detailed in Yahoo's September 9, 2016 preliminary proxy, the Board was actively involved in overseeing the Verizon Transaction, including overseeing negotiations between Yahoo and Verizon. Among other things, the Board oversaw the extensive drafting and "mark-up" process for the relevant transaction agreements, and ultimately approved the agreements, including a Stock Purchase Agreement.

81. Notwithstanding the fact that the Board was well-aware of the [REDACTED] Intrusion and knew that Yahoo had experienced the largest data breach for a single site in history, the Board approved provisions in the Stock Purchase Agreement pursuant to which Yahoo warranted that the Company had experienced no security breaches or thefts of data that could be expected to have a materially adverse effect on the Company's business. Article II, Clause (p) stated:

(p) To the Knowledge of Seller, there have not been any incidents of, or third party claims alleging, (i) Security Breaches, unauthorized access or unauthorized use of any of Seller's or the Business Subsidiaries' information technology systems or (ii) loss, theft, unauthorized access or acquisition, modification, disclosure, corruption, or other misuse of any Personal Data in 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.

82. In other words, the Board approved these warranties knowing they were false. Notably, the transaction agreements (specifically, the Reorganization Agreement) provided that Verizon would assume all liability arising from the core business Yahoo was selling to it, including liabilities “arising from or related to any period prior to” closing of the Verizon Transaction.

83. In late July 2016, Verizon discovered evidence on what is called the “dark web” – an encrypted network of servers often used by hackers – that Yahoo’s security may have been breached and user data stolen. Shortly thereafter, Verizon privately raised with Company management concerns that Yahoo user data had been compromised.

84. By early August 2016, rumors had begun to swirl in the marketplace that Yahoo had been the subject of a massive email breach. The Company was thus forced to finally disclose the truth to its users, as it should have done in February 2015 at the latest.

85. Even at this point, however, the Company delayed disclosing the [REDACTED] Intrusion until September 22, 2016 in order to minimize the impact of the adverse news on the Company’s third quarter results. As Benning & Scattergood analysts noted in an October 18, 2016 report, “Rumors of the email breach

surfaced in early August, but the Company did not confirm it until the end of September, which likely mitigated any impact on 3Q16 results.”

86. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED].<sup>3</sup> (Ex. 14.)

87. [REDACTED]

[REDACTED] (*Id.* at YHOO S’holder Demand 003670-79.)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] (*Id.* at YHOO S’holder Demand 003680-861.)

---

<sup>3</sup>

[REDACTED]

88. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

89. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] (*Id.* at YHOO S’holder Demand 003862-869.) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

**VII. YAHOO FINALLY DISCLOSES THE [REDACTED] INTRUSION TO USERS AND TO VERIZON.**

90. On September 22, 2016, Yahoo issued a press release finally acknowledging the [REDACTED] Intrusion. In the press release, the Company stated that in “late 2014 . . . information associated with at least 500 million user accounts was stolen” from the Company’s network “by what [Yahoo] believes is a state-sponsored actor.”

91. Yahoo’s press release did not mention that the Company, its Board, and the Audit and Finance Committee had known about the [REDACTED] Intrusion since at least early 2015, and misleadingly suggested that the Company had first learned about the attack through “[a] recent investigation.” [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

92. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] (Ex. 15,

at YHOO S’holder Demand 003942-4299.) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] (Ex. 16.)

93. As discussed further below, Yahoo was widely criticized in the wake of its September 22, 2016 announcement for the apparent delay in disclosing the

█████ Intrusion, and this criticism has led to a significant erosion in the Company's good will. In particular, commentators, and even Congressmen, pointed to the unusual length of time it supposedly took the Company to "discover" the hack.

94. Given the extraordinary length of time that has elapsed between the █████ Intrusion and the Company's disclosure, Senator Mark Warner raised the possibility that Yahoo had failed to comply with the SEC's Guidance Concerning Cyber Security Incident Disclosure. Likewise, in a statement calling for a Congressional probe, Senator Richard Blumenthal stated, "If Yahoo knew about the hack as early as August, and failed to coordinate with law enforcement, taking this long to confirm the breach is a blatant betrayal of their users' trust." Little did Senator Blumenthal know, the Board knew of the █████ Intrusion since early June 2015 at the latest.

95. Media reports and commentators also noted that the length of time between the occurrence and disclosure of the █████ Intrusion indicated that Yahoo had improperly concealed the event. For instance, a September 23, 2016 *Fortune* article reported that "[t]here is strong evidence Yahoo knew about the attack for well over a month, and possibly much longer . . . . Instead of promptly



telling everyone to change their password, Yahoo appears to have just sat on the information.”

96. Similarly, an article in the *Financial Times* noted that the Company’s press release disclosing the [REDACTED] Intrusion was issued “only 13 days after the [C]ompany issued a statement to the Securities and Exchange Commission that said it had no knowledge of ‘any incidents’ of ‘security breaches, unauthorised [sic] access or unauthorised [sic] use’ of its IT systems.” The article also quoted Forrester securities analysts, who stated, “It’s taken almost two years for Yahoo to discover, verify, come clean, and inform [users] — which is absolutely unacceptable in 2016.”

97. Yahoo’s delay in disclosing the [REDACTED] Intrusion has also attracted the attention of regulators. The FBI, SEC, and FTC have all commenced investigations to determine whether the Company improperly concealed the [REDACTED] Intrusion.

98. Finally, Verizon has indicated that Yahoo’s belated disclosure has significantly prolonged the process for closing the Verizon Transaction. For instance, on an October 20, 2016 earnings call with investors, Verizon’s then-CFO, Fran Shammo, stated that reevaluating Verizon’s position in light of Yahoo’s

disclosure would be “a long process” and that “it’s going to take some time to evaluate this.”

99. The extent of the delay demonstrates that Verizon was concerned not only about the integrity of Yahoo’s security systems, but about the Board’s apparent failure to be forthcoming about the hack to users, and the consequences of this unlawful concealment.

100. This wave of adverse news, engendered by the Board’s failure to disclose the [REDACTED] Intrusion for almost two years after learning about it, has significantly harmed Yahoo’s reputation and diminished its good will.

101. Astonishingly, on December 14, 2016, Yahoo disclosed that the data Verizon had brought to its attention in July of 2015 indicated that the Company had been the victim of another major cyberattack in August 2013. Yahoo further disclosed that this 2013 attack had compromised more than 1 billion user accounts. In light of the paucity and limited scope of the Company’s production in response to Plaintiff’s Section 220 demands, only further discovery (including depositions) can determine whether the reports about [REDACTED] made to the Board included detail about the August 2013 cyberattack as well.

**VIII. YAHOO AND ITS STOCKHOLDERS HAVE SUSTAINED SIGNIFICANT HARM AS A RESULT OF THE BOARD'S BREACHES OF FIDUCIARY DUTY.**

102. As a direct and proximate result of the Board's breaches of its fiduciary duties, Yahoo and its shareholders have sustained, and continue to sustain, significant harm arising from its failure to disclose the [REDACTED] Intrusion to both the Company's users and to Verizon.

103. *First*, as discussed above, the Board's failure to timely disclose the [REDACTED] Intrusion to its users exposed the Company to the threat of significantly expanded legal liability under UDAAP and similar state laws. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

104. Accordingly, by declining to disclose the [REDACTED] Intrusion when it was first brought to the Company's attention, Yahoo and its Board knowingly exposed users to both the threat of continued harmful and improper use of their personal information and ongoing and additional intrusions for at least a year and a half. The Board's attempt to cover up the attack, rather than publicly acknowledge the intrusion and allow users to take action to mitigate the hack's impact,

significantly compounds the Company's potential legal liability and exposes the Company to treble or punitive damages.

105. The Board's misconduct has also exposed the Company to adverse regulatory action. As discussed above, the FBI, SEC, FTC, and even members of Congress, have announced investigations into Yahoo's delay in disclosing the [REDACTED] Intrusion.

106. *Second*, the Board's conduct in concealing the [REDACTED] Intrusion from its users has significantly eroded Yahoo's good will, making it likely that Yahoo will be forced to accept significantly adverse changes to the terms of the sale of its operations in the Verizon Transaction.

107. Verizon itself has indicated that Yahoo's delay in disclosing the [REDACTED] Intrusion clearly damaged the Company's value, and that this damage ought to be reflected in the purchase price. On an October 20, 2016 earnings call with investors, Verizon's then-CFO, Fran Shammo, responded affirmatively to an analyst's question about whether the breach constituted a "material adverse condition" that would allow Verizon to terminate or renegotiate the Verizon Transaction. Shammo also emphasized that at a minimum, the breach would significantly delay consummation of the deal. Shammo stated, "This was an extremely large breach that has received a lot of attention from a lot of different

people, so we have to assume that it will have a material impact on Yahoo. Lawyers had their first call yesterday with Yahoo to provide us information, but from what I understand that's going to be a long process. So unless Yahoo comes up with different process, it's going to take some time to evaluate this."

108. Originally, market commentators and analysts reported that Verizon was seeking to discount the \$4.8 billion deal price by as much as \$1 billion – more than 20%. It is clear that this discount represents, at least in part, additional legal liability incurred during the year and a half the Board failed to disclose the hack and good will lost as a consequence of Yahoo's extraordinary delay. A discount of that magnitude is also consistent with market expectations: in the wake of Yahoo's September 22, 2016 announcement, Yahoo stock fell from \$44.15 per share to \$42.80, erasing roughly \$1.3 billion in market capitalization.

109. Analysts likewise expressed trepidation about the concessions Verizon might seek as a result of the Yahoo's delay in disclosing the [REDACTED] Intrusion and consequent loss of good will. For instance, in an October 19, 2016 report Credit Suisse analysts expressed concern over "the unanswered question of what steps Verizon may take to renegotiate the terms of the deal given the now highly publicized data breach at Yahoo." Likewise, in an October 21, 2016 report Jeffries analysts worried:

We have additional uncertainty around the closing of VZ's acquisition of Yahoo's core business given the revelation of an email hack in 2014 that exposed 500MM users' information. We believe that VZ could rule this as a material issue that was not revealed during due diligence. It has been reported by major news outlets that VZ could be looking for a \$1B discount or might even walk away from the deal. If the later transpires we believe YHOO shares would be under additional pressure. If the deal falls apart Yahoo may be required to pay VZ a fee of \$144.8MM if deemed a material breach of the purchase agreement.

110. On February 17, 2017, *The New York Times* reported that Yahoo is close to renegotiating its original deal, choosing to take close to \$300 million off the deal price to preserve the sale. While the \$300 million price reduction is less than market analysts originally expected, Yahoo agreed to additional concessions that ultimately will result in significant future liability.

111. As noted above, Verizon originally agreed to assume any legal liability relating to Yahoo's core business. However, *The New York Times* has now reports that the revised deal terms contemplate having the two companies share legal responsibility and costs for the data breaches.

112. Given the magnitude of the [REDACTED] Intrusion, and the Company's willful failure to disclose the existence of the data breach, Yahoo's legal liability will likely far exceed the \$300 million in concrete damages that the Company is already on the verge of incurring as a result of the revised deal price.

**THE UTILITY AND LIMITATIONS OF THE PLAINTIFF'S**  
**SECTION 220 BOOKS AND RECORDS DEMAND**

113. Plaintiff here did not simply rest on the Company's public disclosures and publicly available information, even though those facts speak for themselves.

114. Rather, following the guidance of the Delaware Supreme Court, Plaintiffs pursued their rights under Section 220 of the Delaware General Corporations Law. In making the Section 220 demand, Plaintiff expressly requested production of Board Materials to determine what the Individual Defendants knew (and when) about the largest security breach in history for a single website. The Section 220 demand defined "Board Materials" broadly to include any Board or committee minutes and materials relating to the Board's approval, monitoring, or oversight of the misconduct alleged herein.

115. Following receipt of two limited productions in response to Plaintiff's demand, Plaintiff sent a deficiency letter seeking core books and records that the Company failed to produce. The Company produced a supplemental production on February 2, 2017. Defendants also provided a response to the deficiency letter,

[REDACTED]

[REDACTED]

116. But the Company's response is more of the same, showing active attempts to not document the most incriminating information the Board discussed.

[REDACTED]

117. Moreover, the Company took the position that certain minutes requested by Plaintiff had not been approved by the Board and/or its committees. Surprisingly, many of these meeting had taken place almost nine months ago. The failure to produce core books and records, and the delay in the Board's approval of such minutes, raises serious concerns that the 220 production is not complete.

118. [REDACTED] have a pattern of providing descriptive information regarding remedial steps in response to cybersecurity threats, but only provide cursory labels when discussing actual cybersecurity breaches at the Company (*e.g.*, [REDACTED] and [REDACTED]. The lack of description relating to highly relevant information is consistent the allegations herein – *i.e.*, that the Board and its committees deliberately concealed and/or drafted these materials in such a way as



to protect the Board and its committees from liability. This is not how fiduciaries should (nor do) oversee legal compliance at Delaware companies.

119. Defendants have reserved their rights to argue that all documents produced in response to the Section 220 demand are incorporated by reference. Due process and fair and just principles of equity cannot permit Yahoo, which has whitewashed board and committee materials and otherwise failed to produce highly relevant information, to receive the benefit of incorporation by reference. Put another way, when Yahoo has the opportunity to “cherry-pick” items in its sole custody and control, while providing a limited and artificially circumscribed production of books and records, Plaintiff has a constitutional right against the Court treating such production as if it were complete or reliable. Only full Rule 26 discovery would provide a basis for the Court to weigh contested facts.

120. Finally, given the continued concealment of the extent of the Board’s knowledge of the [REDACTED] intrusion, and in light of the requirement in the Company’s Board and Committee charters’ to keep accurate records of any Board and committee meetings, Plaintiff is entitled to receive the benefit of all reasonable inferences drawn from the glaring absence in the production of the relevant core books and records identified above – books and records that the Company should have readily possessed and produced.

### **DERIVATIVE ALLEGATIONS**

121. Plaintiff brings this action derivatively in the right and for the benefit of Yahoo to redress the breaches of fiduciary duty and other violations of law by the Individual Defendants, as alleged herein.

122. Plaintiff has owned Yahoo common stock continuously since at least September 30, 2013, and will continue to hold Yahoo common stock throughout the remainder of this action.

123. Plaintiff will adequately and fairly represent the interests of Yahoo and its stockholders in enforcing and prosecuting the Company's rights, and Plaintiff has retained counsel experienced in prosecuting this type of derivative action.

124. Plaintiff has not made a pre-suit demand on the Board to assert the claims set forth herein against the Individual Defendants because such a demand would have been futile, and thereby is excused because the allegations herein, at a minimum, permit the inference that the directors lack the requisite independence and disinterest to determine fairly whether these claims should be pursued.

### **DEMAND FUTILITY**

125. Yahoo's Board at the time this action was initiated consisted of the following directors: Braham, Brandt, Filo, Friedman, Hartenstein, Hill, Mayer,

McInerney, Shaw, Smith, and Webb. Plaintiff has not made any demand on the Board to institute this action against the Defendants because, for the reasons set forth below, such demand would be a futile and useless act.

126. Under Delaware law, a fiduciary's decision to knowingly violate the law cannot constitute a valid business judgment. Here, Defendants willfully concealed the existence of a security breach in direct violation of the Company's own policies as well as provisions of state law. Moreover, Defendants were on notice of the Company's legal obligation to notify users of security breaches. Further, here, Defendants also had a heightened duty to be truthful when negotiating the sale of substantially all the Company's assets.

127. Here, demand on the Board is futile because, consistent with the Company's reporting mechanisms outlined in the Corporate Governance Guidelines and the Audit and Finance Committee chart, a majority of the Board had knowledge of and received repeated updates regarding the [REDACTED] Intrusion starting in October 2014 and continuing until at least April 2016. Knowledge of the [REDACTED] Intrusion is based on a review of the Company's core books and records, including:

a) [REDACTED]

b)

c)

d)

128. As evidenced by statements in the Company's public filings, previous course of conduct relating to similar security breaches, and internal company policies and procedures, the Board knew that the Company had a legal obligation to comply with these state laws, including their requirement to notify users of suspected security breaches. Notwithstanding its knowledge of the [REDACTED]

Intrusion, the Board and the Audit and Finance Committee failed to disclose the Intrusion to its users for nearly two years, in violation of applicable law. This willful delay in notifying users of security breaches has significantly increased the Company's legal liability under UDAAP and similar consumer protection laws, and has eroded the Company's good will. As a result, demand is futile because a majority of the Board faces a substantial likelihood of liability.

129. Demand on the Board is also futile because the Board caused the Company to agree to provisions in the Stock Purchase Agreement in which Yahoo represented and warranted that the Company had experienced no security breaches or thefts of data that could be expected to have a materially adverse effect on the Company's business. The Board and the Audit and Finance Committee had knowledge of and received repeated updates regarding the [REDACTED] Intrusion, which represented the largest data breach in history for a single website, and therefore was patently material to the Company's business. By entering into the Stock Purchase Agreement with knowledge of the [REDACTED] Intrusion as recently as April 2016, the Board breached its fiduciary duties by concealing the security breach. The Board's decision to engage in concealment was made in bad faith and was not otherwise the product of a valid business judgement. As a result, demand is futile because the Board faces a substantial likelihood of liability.

130. Demand is also futile because the Board continues to conceal the full extent of the Board's and the Audit and Finance Committee's knowledge of the [REDACTED] Intrusion in breach of its fiduciary duties. The Board continues to allow the Company to conceal the extent of the Board's and the Audit and Finance Committee's knowledge of the [REDACTED] Intrusion, [REDACTED]

[REDACTED]

[REDACTED] ry

[REDACTED]

131. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

132. By concealing these facts, the Board continues to allow the Company to mislead users, Verizon, and stockholders in breach of their fiduciary duties. The

Board's decision to conceal this information was not done in good faith and was not otherwise the product of a valid business judgement. As a result, demand is futile because the Board faces a substantial likelihood of liability.

133. Demand is also futile as to Defendants Mayer and Filo because neither is independent. Defendant Mayer is employed with the Company as Chief Executive Officer. Defendant Filo is employed with the Company as Chief Financial Officer. In the Company's most recent Proxy Statement, filed on May 23, 2016, the Company admits that "Ms. Mayer and Mr. Filo are not independent." Given the highly detailed information presented to the Board concerning the [REDACTED] Intrusion, the reasonable inference exists that senior executives received full disclosure of this information in management meetings. As such, demand is futile as to these directors for this additional reason.

## **COUNTS**

### **COUNT I**

#### **Breach of Fiduciary Duty (Against the Director Defendants)**

134. Plaintiff incorporates by reference and realleges each and every allegation set forth above, as though fully set forth herein.

135. Under Delaware law, the Director Defendants (all directors of Yahoo) each owed and continue to owe fiduciary duties to Yahoo and its stockholders. By reason of their fiduciary relationships, the Director Defendants specifically owed

and owe Yahoo the highest obligation of good faith and loyalty in the administration of the Company, including, without limitation, the duty to not allow Yahoo to violate laws governing the prevention and detection of security breaches, the obligation to notify users and disclose such breaches in a timely fashion and in good faith, and the duty to refrain from knowingly and actively concealing the existence of such breaches from users, stockholders, and potential acquirors.

136. In addition, the Director Defendants have specific fiduciary duties as defined by the Company's corporate governance documents, including the Corporate Governance Guidelines and the charter of the Audit and Finance Committee; principles that, had they been discharged in accordance with the Director Defendants' obligations, would have necessarily prevented the misconduct and consequent harm to the Company alleged herein.

137. The Director Defendants consciously breached their fiduciary duties and otherwise violated their corporate responsibilities in at least the following ways:

- a) Knowingly and repeatedly failing to disclose a massive security breach to users for more than two years in violation of law;
- b) Willfully causing the Company agree to representations and warranties that the Company had already materially breached;



- c) Actively concealing the Board's and the Audit and Finance Committee's knowledge of a massive security breach, including the date and extent of such knowledge; and
- d) Knowingly causing the Company to issue materially false and misleading statements to its users, stockholders, and Verizon.

138. As a direct and proximate result of the Director Defendants' conscious failure to perform their fiduciary duties, Yahoo has sustained and will continue to sustain significant damages – both financially and to its corporate image and good will. Such damages to Yahoo caused by the Director Defendants include, and will include, the substantial penalties, fines, damages awards, settlements, expenses, and other liabilities described herein. Moreover, Yahoo is currently in re-negotiating with Verizon the Company's \$4.8 billion deal to sell substantially all the Company's assets. As a result of the Director Defendants' misconduct, the Company faces expanded legal liability to its users, has suffered loss of good will, and stockholders have suffered delayed receipt of valuable consideration in connection with the Verizon Transaction.

139. As a result of the misconduct alleged herein, the Director Defendants are liable to the Company.

**COUNT II**  
**Breach of Fiduciary Duty**  
**(Against Defendants Mayer and Filo In Their Capacities As Officers)**

140. Plaintiff incorporates by reference and realleges each and every allegation set forth above, as though fully set forth herein.

141. Under Delaware law, Defendants Mayer and Filo, acting in their capacities as Chief Executive Officer and Chief Financial Officer, respectively, owed and continue to owe fiduciary duties to Yahoo and its stockholders. By reason of their positions as an executive officer of the Company, Defendants Mayer and Filo owed duties of due care, good faith, and loyalty. Defendants Mayer and Filo were duty-bound to exercise that degree of care that a reasonably prudent officer would use under the circumstances and, moreover, to faithfully and honestly pursue the lawful best interest of Yahoo.

142. Defendants Mayer and Filo consciously breached their fiduciary duties and otherwise violated their corporate responsibilities in at least the following ways:

- a) Knowingly and repeatedly failing to disclose a massive security breach to users for more than two years in violation of law;
- b) Willfully causing the Company agree to representations and warranties that the Company had already materially breached;

- c) Actively concealing the Board's and the Audit Committee's knowledge of a massive security breach, including the date and extent of such knowledge; and
- d) Knowingly causing the Company to issue materially false and misleading statements to its users, stockholders, and Verizon.

143. As a direct and proximate result of the Defendants Mayer's and Filo's conscious failure to perform their fiduciary duties, Yahoo has sustained and will continue to sustain significant damages – both financially and to its corporate image and good will. Such damages to Yahoo caused by Defendants Mayer and Filo include, and will include, the substantial penalties, fines, damages awards, settlements, expenses, and other liabilities described herein. Moreover, Yahoo is currently in discussions with Verizon to re-negotiate the Company's \$4.8 billion deal to sell substantially all the Company's assets. As a result of Defendants Mayer's and Filo's misconduct, the Company faces expanded legal liability to its users, has suffered loss of good will, and stockholders have suffered delayed receipt of valuable consideration in connection with the Verizon Transaction.

144. As a result of the misconduct alleged herein, the Director Defendants are liable to the Company.

## **PRAYER FOR RELIEF**

**WHEREFORE**, Plaintiffs demand judgment as follows:

- a. determining that this action is a proper derivative action maintainable under the law and demand was excused;
- b. finding that Defendants breached their fiduciary duties by concealing the [REDACTED] Intrusion in violation of federal and state laws and regulations;
- c. against all Defendants and in favor of the Company for the amount of any and all damages sustained by Yahoo as a result of Defendants' breaches of fiduciary duties, including any and all damages compensable by statute and/or law;
- d. against all Defendants and in favor of the Company for extraordinary equitable and injunctive relief as permitted by law and/or equity;
- e. directing Yahoo to take all necessary actions to reform and improve its compliance procedures and governance policies to comply with applicable laws and to protect Yahoo and its stockholders from a repeat of the damaging events described herein;
- f. awarding to Plaintiff the costs and disbursements of the action, including reasonable attorneys' fees, accountants', consultants' and experts' fees, costs, and expenses; and
- g. granting such further relief as the Court deems just and proper.

FRIEDLANDER & GORRIS P.A.

/s/ Joel Friedlander

Joel Friedlander (Bar No. 3163)  
Christopher M. Foulds (Bar No. 5169)  
Christopher P. Quinn (Bar No. 5823)  
1201 N. Market Street, Suite 2200  
Wilmington, DE 19801  
(302) 573-3500

*Counsel for Plaintiff*

OF COUNSEL:

Mark Lebovitch  
David Wales  
Abe Alexander  
David MacIsaac  
BERNSTEIN LITOWITZ BERGER  
& GROSSMANN LLP  
1251 Avenue of the Americas  
New York, NY 10020  
(212) 554-1400

Dated: February 20, 2017