POMERANTZ LLP
Jeremy A. Lieberman (pro hac vice)
Emma Gilmore (pro hac vice)
Michael Grunfeld (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 THIS DOCUMENT RELATES TO: ALL ACTIONS	Case No. 17-CV-00373 (LHK) **SECOND AMENDED CLASS ACTION COMPLAINT FOR VIOLATIONS OF THE FEDERAL SECURITIES LAWS** JURY TRIAL DEMANDED

TABLE OF CONTENTS

Lead Plaintiffs Ben Maher ("Maher") and Sutton View Partners LP ("Sutton View"), and named plaintiff Nafiz Talukder ("Talukder") (collectively, "Plaintiffs"), on their behalf and on behalf of all other persons similarly situated, by Plaintiffs' undersigned attorneys, for Plaintiffs' complaint against Defendants (defined below), allege the following based upon personal knowledge as to Plaintiffs and Plaintiffs' own acts, and information and belief as to all other matters, based upon, *inter alia*, the investigation conducted by and through Plaintiffs' attorneys, which included, among other things, a review of the Defendants' public documents, conference calls and announcements made by Defendants, United States Securities and Exchange Commission ("SEC") filings, federal indictments, wire and press releases published by and regarding Yahoo! Inc. ("Yahoo" or the "Company"), analysts' reports and advisories about the Company, information readily obtainable on the Internet, and documents obtained in the shareholder class action litigation against Yahoo, including documents that were produced in response to a demand for corporate books and records pursuant to Section 220 of the Delaware General Corporations Law and in response to expedited discovery. Plaintiffs believe that substantial evidentiary support will exist for the allegations set forth herein after a reasonable opportunity for discovery.

NATURE OF THE ACTION

1. This is a federal securities class action on behalf of a class consisting of all persons other than Defendants who purchased or otherwise acquired Yahoo securities between April 30, 2013 and December 14, 2016, both dates inclusive (the "Class Period"). Plaintiffs seek to recover compensable damages caused by Defendants' violations of the federal securities laws and to pursue remedies under Sections 10(b) and 20(a) of the Securities Exchange Act of 1934 (the "Exchange Act") and Rule 10b-5 promulgated thereunder.

2. This action involves Defendants' brazen failure to disclose the two largest data breaches in U.S. history, in which hackers stole the records of *three billion users* in 2013[1] and compromised the accounts of 500 million users in 2014 and caused financial harm to its investors. Defendants also failed to disclose two additional massive data breaches in 2015 and 2016, which affected approximately 32 million Yahoo users and caused financial harm to its investors. Throughout the Class Period, Defendants fraudulently reassured the public that Yahoo had "physical, electronic, and procedural safeguards that comply with federal regulations to protect personal information about [its users]," that it would publicly disclose all security vulnerabilities within 90 days of discovery, and that its data security employed "best practices," among other misrepresentations. Meanwhile, Defendants knew but failed to disclose that Yahoo was employing grossly outdated and substandard information security methods and technologies, which had resulted in two of the largest data security breaches in history.

3. Yahoo's products and services involve the storage and transmission of Yahoo's users' and customers' personal and proprietary information, including the users' names, email addresses, telephone numbers, birth dates, passwords, social security numbers, security questions linked to a user's account, and credit and/or debit card information. Yahoo trumpets its access to users' private information in an effort to appeal to advertisers through its ability to conduct targeted advertisements. While a user's

---

[1] On October 3, 2017, Verizon – which acquired most of Yahoo's operating businesses in June 2017 – belatedly announced that the 2013 data breach actually affected *all three (3) billion of Yahoo's user accounts* – three times the amount originally disclosed by Yahoo. *See, e.g.*, Nicole Perlroth, "All 3 Billion Yahoo Accounts Were Affected by 2013 Attack," THE NEW YORK TIMES (Oct. 3, 2017). The article noted that "Yahoo maintains that the breaches in 2014 and 2013 are not related. But investigators believe the attackers behind the 2013 breach were Russian and possibly linked to the Russian government." As demonstrated *infra*, the information contemporaneously available to and known by Defendants in 2014 and 2015—including the hackers' compromise of the user database ("UDB")—was sufficient to alert Defendants to the fact that *all* users had been affected since the UDB contained the information about *all* Yahoo's users.

On October 5, 2017, in the related consumer data privacy class action also consolidated before this Court, the Court issued *sua sponte* an "Order Re: Yahoo Recent Data Breach Disclosure," requiring Defendant Yahoo/Altaba to produce on an expedited basis information relating to the recent disclosure that the 2013 data breach had affected 3 billion user accounts.

private information is indispensable and the most valuable asset to Yahoo's business, it is also "as good as gold" to identity thieves, who exploit it for a variety of nefarious reasons, including draining the bank accounts of the victims whose information they misappropriated, claiming their disability benefits, obtaining a driver license in their name, and committing tax fraud.

4. During the Class Period, Yahoo repeatedly warned in its public filings that cybersecurity attacks represented a material operating risk, warning 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." Understanding the gravity of identity theft, Defendants publicly acknowledged that "there is nothing more important to [Yahoo] than protecting our users' privacy." To that end, Yahoo proclaimed on its official website that "[t]ime is of the essence when we discover" security vulnerabilities and "commit[ed] to publicly disclos[e] . . . [on its website] the vulnerabilities we discover within 90 days." Indeed, almost every state in the country makes it illegal for any company to improperly delay notifying customers of data breaches because companies have little to no incentive to disclose hacks voluntarily, given the financial and reputational harm a security breach can cause. Similarly, the Securities and Exchange Commission requires "timely, comprehensive, and accurate information" about cybersecurity incidents, particularly where a registrant experienced a cyber attack compromising customer data.

5. Defendants recently admitted they had contemporaneous knowledge of the breaches: "the Company's information security team had contemporaneous knowledge of the 2014 compromise of user accounts, as well as incidents by the same attacker involving cookie forging in 2015 and 2016. In late 2014, senior executives and relevant legal staff were aware that a state-sponsored actor had accessed certain user accounts by exploiting the Company's management tool."[2] Despite their contemporaneous

[2] Unless otherwise stated, all emphases are added.

knowledge of the massive breaches plaguing Yahoo during the Class Period, Defendants misled investors through their repeated assurances that "Yahoo! takes your privacy seriously," Yahoo has "physical, electronic, and procedural safeguards that comply with federal regulations to protect [users'] personal information," "we implemented the latest in security best-practices," and "the bad guys who [in the past] have used email spoofing to forge and launch phishing attempts . . . were nearly stopped in their tracks," all the while failing to disclose the massive data breaches threatening the privacy and security of all its three billion customers.

6. Defendants had every reason to keep the breaches under wraps. The concealment enabled Yahoo to maintain its user base and a needed stream of revenues at a time when the Company's financial performance was severely deteriorating. For example, while all online advertising revenue in the U.S. increased by 16.9% year over year in Q3 2014 to $12.4 billion, Yahoo's gross advertising revenues declined by 1.3% to 4.61 billion. This lackluster performance prompted repeated calls for Yahoo to sell itself. But even as it was finalizing a sale of its core business to Verizon in 2016, Yahoo falsely represented in a regulatory filing on September 9, 2016, that "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 Yahoo's possession. Since the breaches came to light, Verizon has threatened to walk out of the deal. More recently, Verizon has successfully renegotiated a $ 350 million price reduction and has required Yahoo to pay 50% of post-closing cash liabilities related to the data breaches.

7. Yahoo's silence in the face of a duty to disclose angered not only investors, but U.S. senators as well, who called the Company's conduct "unacceptable" and questioned its "truthfulness in representations to the public." When the market learned of the data breaches through a series of

corrective disclosures, Yahoo's shares plummeted by over 31%, significantly harming investors. Moreover, during the Class Period, Yahoo's core business declined by billions of dollars, leaving investors exposed to inaccurate assumptions as a result of Defendants' failure to disclose the data breaches, and inflicting additional harm on investors.

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

JURISDICTION AND VENUE

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

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

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

12. In connection with the acts, conduct and other wrongs alleged in this Complaint, Defendants, directly or indirectly, used the means and instrumentalities of interstate commerce, including but not limited to, the United States mail, interstate telephone communications and the facilities of the national securities exchange.

PARTIES

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

14. Defendant Yahoo! Inc. is incorporated in Delaware, and the Company's principal executive offices are located at 701 First Avenue, Sunnyvale, California, 94089. During the Class Period, Yahoo's common stock traded on the NASDAQ under the ticker symbol "YHOO." Yahoo! is presently known as Altaba.[3]

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

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

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

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

[3] On July 25, 2016, Yahoo announced that it had entered into an agreement to sell its operating business to Verizon (the "Sale Transaction"), subject to approval by Yahoo's shareholders. The Shareholders voted to approve the Sale Transaction on June 8, 2017, and it closed on June 13, 2017. Following the closing of the Sale Transaction, Yahoo was re-named Altaba, a registered investment company holding stock in Alibaba and Yahoo Japan, plus smaller interests in technology companies like Snap, Inc. Verizon combined the portion of Yahoo it acquired with previously acquired AOL into a subsidiary named Oath.

SUBSTANTIVE ALLEGATIONS

Background

19. Yahoo, together with its subsidiaries, is a multinational technology company that provides a variety of internet services, including, *inter alia*, a web portal, search engine, Yahoo! Mail, Yahoo! News, Yahoo! Finance, sports, advertising, and a microblogging and social networking website, Tumblr. As of February 2016, Yahoo had an estimated 1 billion monthly active users. To utilize Yahoo's services, users must setup user account(s), which requires users to provide Yahoo with private, personal information.

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

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

22. During the Class Period, Yahoo represented that "protecting our systems and our users' information is paramount to ensuring Yahoo users enjoy a secure user experience and maintaining our users' trust."[4] Yahoo vouched that "[w]e have physical, electronic, and procedural safeguards that

[4] Security at Yahoo, Yahoo!, https://policies.yahoo.com/us/en/yahoo/privacy/topics/security/index.htm.

comply with federal regulations to protect personal information about you."[5]

Private Information Is Valuable to Criminals

23. It is well known and the subject of many media reports that Private Information is highly coveted and a frequent target of hackers. Legitimate organizations and criminals alike recognize the value of Private Information. Otherwise, they would not aggressively seek or pay for it. For example, in "one of 2013's largest breaches [involving a leading software company] . . . not only did hackers compromise the [card holder data] of three million users, they also took registration data from 38 million users."[6] Similarly, in the data breach of Target Corporation, between November 27 and December 15, 2013, hackers stole personal information of as many as 70 million people, including customer names, mailing addresses, phone numbers, credit or debit card numbers, and the card's expiration date and CVV (card verification value). "Increasingly, criminals are using biographical data gained from multiple sources to perpetrate more and larger thefts."[7]

24. Private Information is "as good as gold" to identity thieves, in the words of the Federal Trade Commission ("FTC").[8] Identity theft occurs when someone uses another's personal identifying information, such as that person's name, address, credit card number, credit card expiration date, and other information, without permission, to commit fraud or other crimes. The FTC estimates that as many as 10 million Americans have their identities stolen each year. As the FTC recognizes, once identity thieves have private information, "they can drain your bank account, run up charges on your credit cards,

[5] *Id.*

[6] Verizon 2014 PCI Compliance Report, http://www.nocash.info.ro/wp-content/uploads/2014/02/Verizon_pci-report-2014.pdf (hereafter "2014 Verizon Report"), at 54.

[7] *Id.*

[8] FTC Interactive Toolkit, Fighting Back Against Identity Theft, http://www.dcsheriff.net/community/documents/id-theft-tool-kit.pdf.

open new utility accounts, or get medical treatment on your health insurance."[9]

25. According to Javelin Strategy and Research, "1 in 4 data breach notification recipients became a victim of identity fraud."[10] Nearly half (46%) of consumers with a breached debit card became fraud victims within the same year.

26. Identity thieves can use Private Information to perpetrate a variety of crimes. For instance, they may commit various types of fraud upon the U.S. government, such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

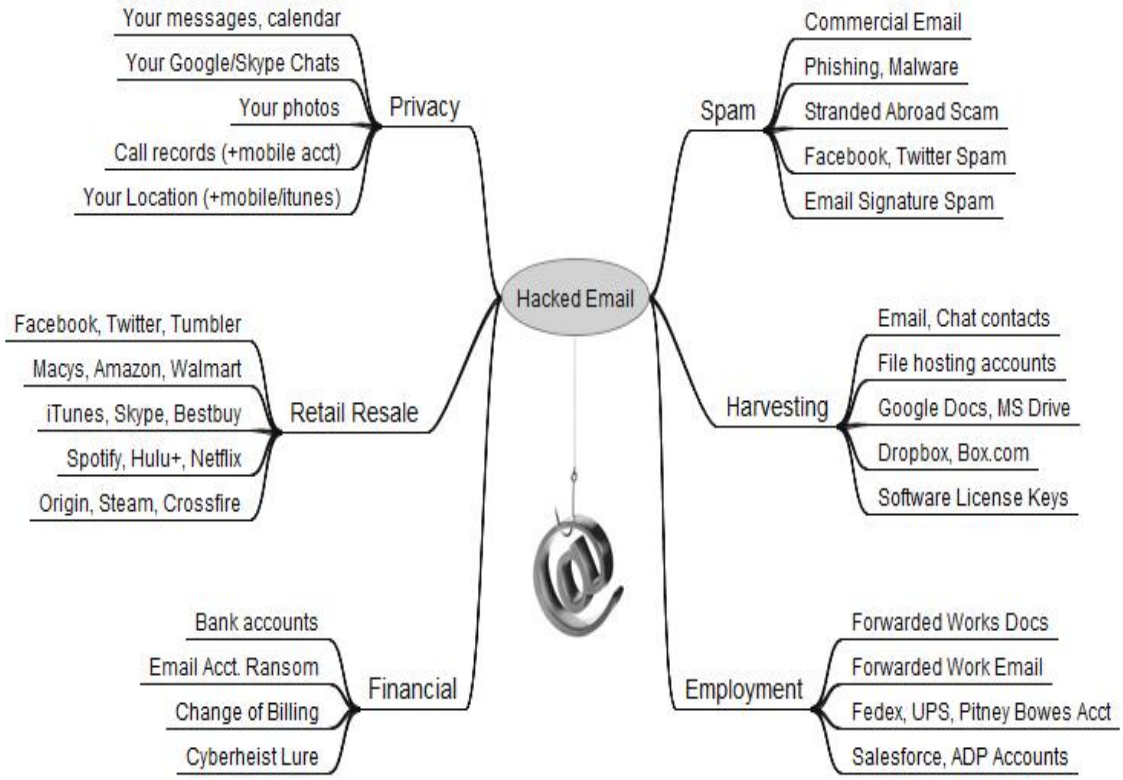
27. Additionally, identity thieves may obtain medical services using consumers' compromised private information or commit any number of other frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest.

28. As depicted in the chart below, a hacked email account gives criminals access to a treasure trove of Private Information:[11]

[9] FTC, Signs of Identity Theft, available at http://www.consumer.ftc.gov/articles/ 0271-signs-identity-theft.

[10] 2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters, http://www.javelinstrategy.com/brochure/276 (the "2013 Identity Fraud Report").

[11] 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.



29. According to Steve Grobman, chief technology officer for Intel Security, email accounts are a jackpot for criminals, as they often contain passwords for financial and workplace accounts, information about investments, and details about the work projects and business plans of anyone from an ordinary person to a CEO, lawyer, or military officer. "The public disclosure of such material could be sensitive enough to destroy careers, enable blackmail, endanger a mission, or influence high-level negotiations and decisions," Grobman said.

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

31. Accordingly, the risks associated with identity theft are grave. "While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out

on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit."[12]

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

> In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of nonfinancial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.[13]

33. Annual monetary losses from identity theft are in the billions of dollars. Javelin Strategy and Research reports that those losses increased to $21 billion in 2013.[14]

34. During the Class Period, Yahoo has repeatedly acknowledged that one of its main operating risks is that of cybersecurity attacks: "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 and financial exposure."

---

[12] True Identity Protection: Identity Theft Overview, http://www.idwatchdog.com/tikia//pdfs/Identity-Theft-Overview.pdf.

[13] 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-identitv-theft-strategic-plan/strategicplan.pdf.

[14] 2013 Identity Fraud Report.

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

> You could be locked out of your online account and be unable to access your e-mail. But there can be even greater consequences. You could be the victim of identity theft.
>
> Once identity thieves have your personal information, the results can be far-reaching, difficult to rectify, and financially devastating.
>
> Armed with your credit card information, fraudsters could charge thousands of dollars to your account before you ever see a statement from your credit card company. They can open new credit card accounts in your name.
>
> Using your identity, they can open a bank account and write bad checks on that account. They can authorize electronic transfers in your name, draining your bank account. To avoid legal action against debts they've incurred using your identity, they might even file for bankruptcy in your name.
>
> They can take out a loan, buy a car, and get a driver's license—all in your name. They may use your name to get a job or file fraudulent tax returns. And if they're arrested, they may give your name to the police and fail to show up for their court date. Then, a warrant for an arrest is issued—in your name.

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

36. Understanding the gravity of security data breaches and the disastrous consequences arising from untimely disclosures of such breaches, Yahoo underscored in its securities filings that almost every state in the country has passed statutes ***making it illegal for any company to improperly delay notifying customers of data breaches***. According to Yahoo's annual filings, "[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." These laws subject violators to significant damages.

37. On its official website, Yahoo represented that:

> ***At Yahoo we take our users' privacy seriously no matter where they are in the world . . . One example of this is our close collaboration over the last year with the Organisation for Economic Cooperation and Development (OECD) as it updated its Privacy Guidelines*** . . . These latest privacy guidelines reference new topics including the strategic importance of national privacy strategies, privacy management programs, and data breach notification . . . ***The OECD's Privacy Guidelines are one of the most commonly referenced privacy frameworks in the world, influencing fair information practices and***

> ***privacy fundamentals in . . . the United States*** . . . Yahoo's Global Public Policy and Privacy teams will continue to engage in efforts like these to help advance privacy frameworks that protect our users . . .

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

> The potential harm to individuals from the misuse of their personal data, whether accidentally lost or purposefully stolen, may be significant.
>
> ***Organisations experiencing a breach often incur significant costs responding to it, determining its cause, and implementing measures to prevent recurrence. The reputational impact can also be significant. A loss of trust or confidence can have serious consequences for organisations. As a result, the security of personal data has become an issue of great concern to governments, businesses and individuals***.
>
> ***Breach notification laws requiring data controllers to inform individuals and/or authorities when a security breach has occurred have been passed*** or proposed in many countries. ***These laws are usually justified on the grounds that data controllers have little incentive to disclose breaches voluntarily, given the possible harm this can cause 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.
>
> Security breaches not only raise privacy concerns, but also intersect with other issues, including criminal law enforcement and cybersecurity. When an organisation suffers a security breach, particularly one resulting from an external attack, notification of the 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.
>
> Requiring notification for every data security breach, no matter how minor, may impose an undue burden on data controllers and enforcement authorities, for limited corresponding benefit. Additionally, excessive notification to data subjects may cause them to disregard notices. Accordingly, the new provision that has been added to the 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***.

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

40. Additionally, as early as October 2011, the SEC has issued guidelines regarding disclosure obligations of filers relating to cybersecurity risks and cyber incidents, in light of the frequent and severe nature of cyber incidents.[15] The SEC emphasized that "the federal securities laws, in part, are designed to elicit disclosure of ***timely, comprehensive, and accurate information*** about risks and events that a reasonable investor would consider important to an investment decision":

> [M]aterial information regarding cybersecurity risks and cyber incidents is required to be disclosed when necessary in order to make other required disclosures, in light of the circumstances under which they are made, not misleading.
>
> **Risk Factors**
>
> Registrants should disclose the risk of cyber incidents ***if these issues are among the most significant factors that make an investment in the company speculative or risky***. In determining whether risk factor disclosure is required, we expect registrants to evaluate their cybersecurity risks and take into account all available relevant information, including prior cyber incidents and the severity and frequency of those incidents. As part of this evaluation, registrants should consider the probability of cyber incidents occurring ***and the quantitative and qualitative magnitude of those risks, including the potential costs and other consequences resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption***. In evaluating whether risk factor disclosure should be provided, registrants should also consider the adequacy of preventative actions taken to reduce cybersecurity risks in the context of the industry in which they operate and risks to that security, including threatened attacks of which they are aware.
>
> Consistent with the Regulation S-K Item 503(c) requirements for risk factor disclosures generally, cybersecurity risk disclosure provided must adequately describe the nature of the material risks and specify how each risk affects the registrant. Registrants should not present risks that could apply to any issuer or any offering and should avoid generic risk

[15] *See* http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

> factor disclosure. Depending on the registrant's particular facts and circumstances, and to the extent material, appropriate disclosures may include . . .
>
> - Description of cyber incidents experienced by the registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences;
>
> - Risks related to cyber incidents that may remain undetected for an extended period . . .
>
> A registrant may need to disclose known or threatened cyber incidents to place the discussion of cybersecurity risks in context. ***For example, if a registrant experienced a material cyber attack in which malware was embedded in its systems and customer data was compromised, it likely would not be sufficient for the registrant to disclose that there is a risk that such an attack may occur***. Instead, as part of a broader discussion of malware or other similar attacks that pose a particular risk, ***the registrant may need to discuss the occurrence of the specific attack and its known and potential costs and other consequences***.[16]

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."[17]

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

[16] *Id.*

[17] *Id.*

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

> In addition to becoming more frequent, there are reports indicating that cyber-attacks have become increasingly costly to companies that are attacked. According to one 2013 survey, the average annualized cost of cyber-crime to a sample of U.S. companies was $11.6 million per year, representing a 78% increase since 2009. In addition, the aftermath of the 2013 Target data breach demonstrates that the impact of cyber-attacks may extend far beyond the direct costs associated with the immediate response to an 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***.
>
> ***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 issued guidance to public companies regarding their disclosure obligations with respect to cybersecurity risks and cyber-incidents. More recently, because of the escalation of cyber-attacks, I helped organize the Commission's March 26, 2014 roundtable to discuss the cyber-risks facing public companies and critical market participants like exchanges, broker-dealers, and transfer agents.
>
> As it has been noted, the primary distinction between a cyber-attack and other crises that a company may face is the speed with which the company must respond to contain the 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.***
>
> While there is no "one-size-fits-all" way to properly prepare for the various ways a cyber-attack can unfold, and what responses may be appropriate, it can be just as damaging to have a poorly-implemented response to a cyber-event. As others have 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***.
>
> ***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)***. In deciding the nature and extent of the disclosures, ***I would encourage companies to go beyond the impact on the company and to also consider the impact on others***. ***It is possible that a cyber-attack may not have a direct material adverse impact on the company itself, but that a loss of customers' personal and financial data could have devastating effects on the lives of the company's customers and many Americans. In***

> ***such cases, the right thing to do is to give these victims a heads-up so that they can protect themselves***.
>
> [B]oard oversight of cyber-risk management is critical to ensuring that companies are taking adequate steps to prevent, and prepare for, the harms that can result from such attacks. There is no substitution for proper preparation, deliberation, and engagement on cybersecurity issues. ***Given the heightened awareness of these rapidly evolving risks, directors should take seriously their obligation to make sure that companies are appropriately addressing those risks***.

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

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

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

> Q: Why does Yahoo disclose security vulnerabilities?
>
> A: Disclosing security vulnerabilities allows everyone to patch their systems. We have to assume that 3rd parties are already aware of these issues or may become aware soon. There is solid evidence that attackers commonly discover and exploit 0-day 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?
>
> A: This depends on the current state of a fix for the vulnerability. If we are in good contact with the party responsible for developing and deploying a fix but they need more time then we reserve the right to extend this deadline as necessary. If we feel no progress is

being made on the fix then we reserve the right to publish the vulnerability details so that the internet community is aware of the issue and individual organizations can defend against or patch it themselves. When this occurs we will do our best to provide mitigation guidance where appropriate. We will make every effort possible to contact all relevant parties and help to coordinate the disclosure when needed.

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

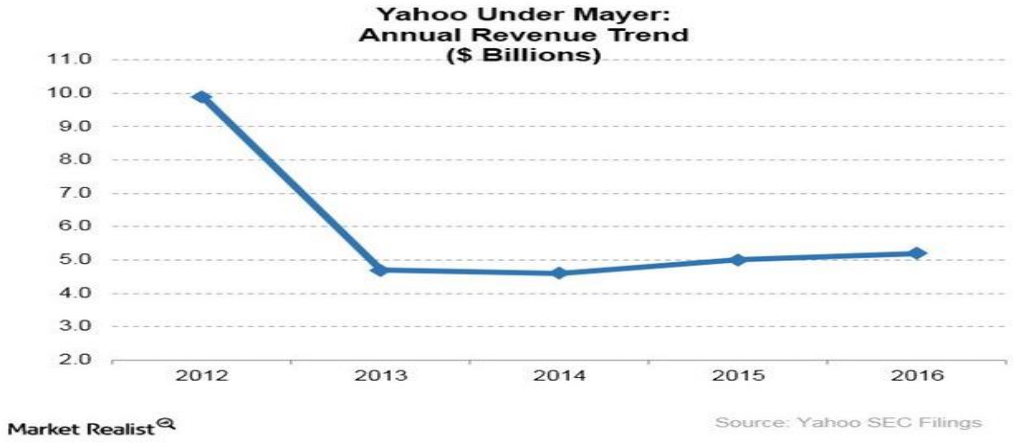
A: Yes. Part of our job is to always be on the lookout for security vulnerabilities that affect the technologies that Yahoo uses and this includes software we didn't develop at Yahoo. These efforts are part of our larger commitment to user security, safety and privacy.

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

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

During the Class Period, Yahoo Struggled to Stay Afloat

46. As measured by annual revenue growth, Defendant Mayer's tenure as Yahoo's CEO was abysmal:[18]



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

48. During the Class Period, Yahoo's stock underperformed the markets. For example, the Company's stock declined by over 17% in the first five months of 2015, while the return on NASDAQ

[18] *See* http://www.nytimes.com/2016/09/29/technology/yahoo-data-breach-hacking.html

composite index was close to 7%. One of the reasons behind Yahoo's lackluster performance was the inability of its core business to deliver the necessary revenue growth from online ads. While online advertising revenue in the U.S. rose by 16.9% year over year in Q3 2014 to $12.4 billion, Yahoo's gross ad revenues declined by 1.3% to 4.61 billion, according to reports by the Interactive Advertising Bureau and PricewaterhouseCoopers US.

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

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

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 (1)(2)	$ 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

[19] *See* http://www.prnewswire.com/news-releases/starboard-delivers-letter-to-ceo-and-board-of-directors-of-yahoo-inc-277223182.html

[20] *Id.*

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":[21]

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
Consolidated	**$ 4,073**	**$ (2,892)**	**$ 1,182**

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.[22]

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."[23]

55. Bowing to pressure from investors unhappy with the eroding financial performance under Mayer's leadership—including the $4.46 goodwill impairment charge taken in 2015 and the hundreds of millions in stock options awarded in 2015 alone—in February 2016, Yahoo officially put itself up for

[21] *Id.*

[22] *Id.*

[23] *Yahoo 'Underperforming' Big-Time, Analyst Says*, Investor's Business Daily, Dec. 10, 2015.

sale. Reportedly, Yahoo gave potential bidders until April 18, 2016 to place their bids. Bidders at the time included Daily Mail, Time Inc., Google, Microsoft, Verizon, and private equity firms General Atlantic, TPG and KKR. If Yahoo did not sell itself, analysts said it could begin "a nasty battle" with Starboard, which threatened to nominate an entirely new slate of directors at Yahoo's next shareholder meeting.

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

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

58. Pursuant to the terms of the 2016 Agreement, the sale to Verizon includes all assets and liabilities of Yahoo's operating business, including Yahoo's products, brands, worldwide offices and business operations, other than a few assets and liabilities identified as Excluded Assets or Retained Liabilities. The Excluded Assets and Retained Liabilities include: all shares in Alibaba Group Holding; all shares in Yahoo Japan, other than commercial arrangements with Yahoo Japan; Yahoo's non-core IP, known as the Excalibur IP portfolio; certain minority investment interests; cash at closing; and Yahoo's

outstanding convertible notes and certain other retained liabilities. Under the 2016 Agreement, Verizon assumed all liability arising from Yahoo's core, operating business, including liabilities "arising from or related to any period prior to" closing of the transaction. With respect to management changes, Yahoo announced that "Verizon and Yahoo will discuss potential integration plans (including reporting structure) between now and closing" and that "post-closing Verizon will determine the leadership structure of the combined entity."

59. Defendant Mayer touted the sale as a significant accomplishment for Yahoo: "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."

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

61. As explained in detail below, by intentionally hiding from investors the massive data breaches that plagued it during the Class Period, the Company was able to attract and maintain users who were duped into believing that Yahoo's services were secure, thus providing the Company with a continuing stream of revenue. This revenue stream was critical for Yahoo at a time when it was struggling amid intense competition. By concealing the data breaches from the public, Yahoo also found a suitor willing to acquire its operating business.

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

62. Yahoo is no stranger to threats against its users' Private Information. However, Yahoo's senior management knew or recklessly ignored that the meager efforts to protect user data were inadequate, despite the fact that its systems were breached time and again for nearly a decade.

63. In 2010, Google informed Yahoo that its systems were being used to attack Google, causing Yahoo to reopen a previously closed security investigation. Yahoo discovered unauthorized access to its systems that predated a 2008 attack that accessed and compromised multiple hosts in Yahoo's corporate network. Yahoo was among the companies whose systems were penetrated by Chinese hackers.

64. As a telling example of Yahoo's inaction, law enforcement authorities notified Yahoo of a potential breach in late 2011. It took Yahoo until about January 30, 2012 to retain an outside security firm, Mandiant, to investigate the breach. Even then, Yahoo evidently did not want to investigate too thoroughly, as it instructed Mandiant not to perform any "Live Response or forensic analysis of any compromised system."

65. Even with investigative limitations, Mandiant conducted its assessment between February 13 and April 3, 2012. Its resulting report on about April 20, 2012 has been characterized as "damning" and identified the earliest evidence of a related intruder on Yahoo's networks as March 22, 2010. Mandiant detected at least two different attack groups in Yahoo's systems, with the most recent activity seen on April 1, 2012. Such information should have caused Yahoo to start to invest in greater security, but Yahoo did no such thing. Yahoo was breached again in 2012.

66. On May 24, 2012, it was reported that with their new Chrome release, Yahoo had inadvertently leaked the private security key that could allow anyone to create malicious plug-ins

masquerading as official Yahoo! Software. Yahoo apologized and released a new version, but the cat was out of the bag, and experts noted that "the implications of the slip have yet to be concluded."

67. On July 11, 2012, over 450,000 unencrypted Yahoo usernames and passwords were stolen and posted on a public website.[24]

68. Yahoo disclosed that breach promptly—the following day.

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

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

71. Yahoo's servers should not have been vulnerable to a SQL injection attack. This type of injection has been known for over a decade and had already been blamed for massive data thefts against Heartland Payment System and others. As far back as 2003, the FTC considered SQL injection attacks

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

to be well-known and foreseeable events that could have and should have been taken into account through routine security measures, which Yahoo failed to adopt.

72. Indeed, "[s]ecurity experts were befuddled . . . as to why a company as large as Yahoo would fail to cryptographically store the passwords in its database. Instead, they were left in plain text, which means a hacker could easily read them."[25] According to a security researcher at Rapid7, Yahoo's security was "definitely poor."[26]

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

> We hope that the parties responsible for managing the security of this subdomain will take this as a wake-up call, and not as a threat … There have been many security holes exploited in Web servers belonging to Yahoo! Inc. that have caused far greater damage than our disclosure. Please do not take them lightly.[27]

74. On November 13, 2012, industry leaders called out Yahoo in a letter to Marissa Mayer demanding encryption: "We urge you to act as quickly as possible on this commitment to user trust and security by taking the long overdue step of deploying HTTPS for all Yahoo! communication services." The stakes were made plain: "Some of us have already been compelled to recommend that users avoid Yahoo! Mail because of its continued lack of essential security protections."

75. On November 23, 2012, it was reported that an Egyptian hacker known as "The Hell" was selling Yahoo stored XSS data. The Hell boasted: "Im [sic] selling Yahoo! stored xss that steal [sic] Yahoo! emails cookies and works on ALL browsers . . . And you don't need to bypass IE or Chrome xss filter as it do [sic] that itself because it's stored xss . . . ."

---

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

[26] *Id*.

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

76. On January 7, 2013, many users reported having their Yahoo! Mail accounts hacked after a hacker named Ramezany uploaded a video demonstrating how to compromise a Yahoo! account by leveraging a DOM-based cross-site scripting (xss) vulnerability exploitable in all major browsers.

77. Rather than strengthening its security team in 2013 – now known to be the year that information for *all* Yahoo accounts was exfiltrated – Yahoo's security staff dropped from 62 employees to 43, including the departure of its Chief Information Security Officer ("CISO"), Justin Somaini. Somaini reportedly left due to disagreements with Defendant Mayer's management style. Yahoo left the position vacant for more than a year, until March 2014.

78. What is more, Yahoo detected multiple security problems throughout 2013, working with outside cybersecurity firms to investigate the issues. Each time, numerous vulnerabilities were identified. Each time, Yahoo hid from rather than fixed its problems.

79. One recurrent problem Yahoo steadfastly refused to fix was the issue of inadequate logging standards. This inadequacy allegedly came up again and again in the security reports prepared for Yahoo. Dell SecureWords ("Dell" or "DSW"), which Yahoo engaged multiple times from 2013 through 2016, allegedly raised the issue with Yahoo repeatedly. During one such 2013 incident, internally dubbed "Project Dickens," data from up to 64 million user accounts appeared to be impacted, with anywhere from 16-23 million involved in a spam email campaign.

80. Based on the spike in spam emails, DSW was retained to investigate potential account compromise in the Yahoo User Database ("UDB") environment.

81. DSW allegedly flagged a very serious vulnerability, but it could not fully evaluate it due to the lack of audit capability on a particular system.

82. Yahoo also retained Leaf SR to conduct a security assessment of Yahoo's UDB environment around the same time in 2013.

83. On or around May 17, 2013, Yahoo Japan was compromised, exposing 22 million Yahoo Japan email addresses.[28] The Company disclosed the breach three days later, asking more than 200 million customers to reset their passwords after detecting an intrusion in one of its main servers. In a press release published on Yahoo Japan's website, Yahoo stressed that it had not confirmed that the data had definitely leaked outside the Company.

84. Yahoo's utter failure to take even the most rudimentary security steps also enabled hackers in late December 2013 to target Java in Yahoo's ad network, infecting roughly 27,000 computers per hour at the time of discovery.[29] Critically, Yahoo's failure also enabled the three massive data breaches that are at the crux of this action: the 2013 Data Breach, the 2014 Data Breach, and the Forged Cookie Data Breach (described below)—the first two widely regarded as ***the biggest data breaches in U.S. history***.

85. The technology industry is rife with similar examples of hackers targeting users' Private Information, including the hacks at Adobe,[30] LinkedIn, eHarmony,[31] and Snapchat,[32] among many others, all of which pre-date the timeframe Yahoo has identified regarding the 2014 Data Breach, and some of which pre-date the 2013 Data Breach. As a company in the online services arena, which employs security professionals, Yahoo undoubtedly knew about these hacks and the high probability that it could suffer similar hacks.

---

[28] Graham Cluley, *22 Million User Ids May Be In The Hands Of Hackers, After Yahoo Japan Security 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-22594136

[29] Andrew Scurria, *European Yahoo Users Victimized In Malware Attack*, Law360 (Jan. 6, 2014), http://www.law360.com/articles/498914 .

[30] *See In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197 (N.D. Cal. 2014).

[31] 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

[32] 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.

86. Despite experiencing the significant data breaches described above, Yahoo knowingly continued to utilize outdated security methods. As reported by Reuters on December 18, 2016, at the time of the 2013 Data Breach, Yahoo used an encryption protocol called MD5 that was considered inadequate by online security professionals. Indeed, a public warning was issued about the inadequacy of MD5 as early as 2008:[33]

> In 2008, five years before Yahoo took action, Carnegie Mellon University's Software Engineering Institute issued a public warning to security professionals through a U.S. government-funded vulnerability alert system: MD5 "***should be considered cryptographically broken and unsuitable for further use***."
>
> Yahoo's failure to move away from MD5 in a timely fashion was an example of problems in Yahoo's security operations as it grappled with business challenges, according to five former employees and some outside security experts. Stronger hashing technology would have made it more difficult for the hackers to get into customer accounts after breaching Yahoo's network, making the attack far less damaging, they said.
>
> "MD5 was considered dead long before 2013," said David Kennedy, chief executive of cyber firm TrustedSec LLC. "Most companies were using more secure hashing algorithms by then."
> He did not name specific firms.

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

88. Yahoo's own security personnel allegedly often relied on external instant and group messaging programs to communicate with each other in order to protect themselves so their communications would not show up on Yahoo's network.

89. As reported by Reuters, former Yahoo security personnel with knowledge of the Company's security protocols told Reuters that "the security team was at times turned down when it requested new tools and features such as strengthened cryptography protections, on the grounds that the

[33] *Yahoo security problems a story of too little, too late*, Reuters (December 18, 2016), http://www.reuters.com/article/us-yahoo-cyber-insight-idUSKBN1470WT

requests would cost too much money, were too complicated, or were simply too low a priority."[34] According to these former Yahoo employees and to outside security experts, "Yahoo's failure to move away from MD5 in a timely fashion was an example of problems in Yahoo's security operations as it grappled with business challenges."[35] "Stronger hashing technology would have made it more difficult for the hackers to get into customer accounts after breaching Yahoo's network, making the attack far less damaging."[36] Yahoo's skimping on security reflected the Company's financial struggles, with revenues steadily falling since their 2008 peak and Yahoo losing its market dominance to its competitors, such as Alphabet Inc.'s Google and Facebook.[37]

90. The former Yahoo employees said "the Company's security problems began before the arrival of Chief Executive Marissa Mayer in 2012 and continued under her tenure. ***Yahoo had suffered attacks by Russian hackers for years, two of the former staffers said***."[38]

91. According to a September 28, 2016 New York Times article based on interviews with several Yahoo insiders who participated in security discussions at Yahoo, "defending against hackers took a back seat at Yahoo." According to those insiders, ***despite knowing during the Class Period that Yahoo was a frequent target for nation-state spies, Defendant Mayer rejected even the most basic security measures and frequently clashed with Yahoo's Chief Information Security Officer "for fear that even something as simple as a password change would drive Yahoo's shrinking email users to other services"***.[39]

---

[34] *Yahoo seen cutting cost corners with security tech discredited long before massive hack*, Reuters, Dec. 19, 2016.

[35] *Id*.

[36] *Id*.

[37] *Id*.

[38] *Id*.

[39] *See* http://www.nytimes.com/2016/09/29/technology/yahoo-data-breach-hacking.html .

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

* * *

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

* * *

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

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

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

The "Paranoids," the internal name for Yahoo's security team, often clashed with other parts of the business over security costs. And their requests were often overridden because of concerns that the inconvenience of added protection would make people stop using the company's products.

* * *

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

* * *

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

* * *

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

Jeff Bonforte, the Yahoo senior vice president who oversees its email and messaging services, said in an interview last December that Mr. Stamos and his team had pressed for Yahoo to adopt end-to-end encryption for everything. Such encryption would mean that

> only the parties in a conversation could see what was being said, with even Yahoo 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.
>
> * * *
>
> ***But when it came time to commit meaningful dollars to improve Yahoo's security infrastructure, Ms. Mayer repeatedly clashed with Mr. Stamos, according to the current and former employees. She denied Yahoo's security team financial resources and put off proactive security defenses, including intrusion-detection mechanisms for Yahoo's production systems. Over the last few years, employees say, the Paranoids have been routinely hired away by competitors*** like Apple, Facebook and Google.
>
> Mr. Stamos, who departed Yahoo for Facebook last year, declined to comment. But during his tenure, ***Ms. Mayer also rejected the most basic security measure of all: an automatic reset of all user passwords, a step security experts consider standard after a breach. Employees say the move was rejected by Ms. Mayer's team for fear that even something as simple as a password change would drive Yahoo's shrinking email users to other services***.[40]

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

93. As a result of the Defendants' refusal to implement appropriate data security safeguards, several prominent Yahoo security experts left the Company during the Class Period. For example, Yahoo's Chief Information Security Officer Alex Stamos left Yahoo for Facebook after repeatedly

[40] *See* http://www.nytimes.com/2016/09/29/technology/yahoo-data-breach-hacking.html .

clashing with Defendant Mayer over security issues. Stamos was hired in 2014 by Yahoo to address security failures, including Yahoo's vulnerabilities to repeated hacks by Russian hackers.[41]

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

> "I believe it to be bigger than what's being reported," the executive, who no longer works for the company but claims to be in frequent contact with employees still there, including those investigating the breach, told Business Insider. "How they came up with 500 is a mystery."
>
> To be sure, Yahoo has said that the breach affected at least 500 million users. But the former Yahoo exec estimated the number of accounts that could have potentially been stolen could be anywhere between 1 billion and 3 billion.
>
> ***
>
> According to this executive, all of Yahoo's products use one main user database, or UDB, to authenticate users. So people who log into products such as Yahoo Mail, Finance, or Sports all enter their usernames and passwords, which then goes to this one central place to ensure they are legitimate, allowing them access.
>
> That database is huge, the executive said. At the time of the hack in 2014, inside were credentials for roughly 700 million to 1 billion active users accessing Yahoo products every month, along with many other inactive accounts that hadn't been deleted.
>
> In late 2013, Yahoo CEO Marissa Mayer said the company had 800 million monthly active users globally. It currently has more than 1 billion.
>
> "***That is what got compromised***," the executive said. "***The core crown jewels of Yahoo customer credentials***."
>
> Yahoo's UDB is still the main repository for user credentials and is still in use, LinkedIn profiles from current Yahoo employees and a 2015 court ruling show.[42]

[41] *Yahoo seen cutting cost corners with security tech discredited long before massive attack*, Reuters, Dec. 19, 2016.

[42] 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 .

95. As investors ultimately learned, the executive was right: Defendants' security breaches impacted three billion Yahoo customers.

The 2013 Data Breach

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

97. As a result, in August 2013, hackers breached the email system of Yahoo, ***stealing the records of all of Yahoo's three 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 forged the cookies that Yahoo places on user computers, including the authentication cookies. By forging the authentication cookies, the hackers could gain access to the targeted accounts without ever having the user's password and would also allow the hacker to remain logged into a user's account indefinitely.

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

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

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

101. Having intercepted the potential sale of the Yahoo database, InfoArmor approached Yahoo through an intermediary to work together, investigate and resolve the massive theft. According to Komarov, instead of leaping into action, ***Yahoo was utterly dismissive*** of the intermediary. At the time, Yahoo was not interested in investigating the breach because it was finalizing a sale of its core business to Verizon in a multi-billion dollar transaction. Yahoo did not want to jeopardize the deal by disclosing the massive breach. Its intermediary having been rejected by Yahoo, InfoArmor notified military and law enforcement authorities in the United States, Australia, Canada, Britain and the European Union about the breach. After those parties verified the authenticity of the stolen records, some of them went to Yahoo directly with their concerns.

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

> Yahoo! Inc. has identified data security issues concerning certain Yahoo user accounts. Yahoo has taken steps to secure user accounts and is working closely with law enforcement.
>
> As Yahoo previously disclosed in November, law enforcement provided the company with data files that a third party claimed was Yahoo user data. The company analyzed this data with the assistance of outside forensic experts and found that it appears to be Yahoo user data. Based on further analysis of this data by the forensic experts, ***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 associated

> with this theft. Yahoo believes this incident is likely distinct from the incident the company disclosed on September 22, 2016.
>
> For potentially affected accounts, the stolen user account information may have included names, email addresses, telephone numbers, dates of birth, hashed passwords (using MD5) and, in some cases, encrypted or unencrypted security questions and answers. The investigation indicates that the stolen information did not include passwords in clear text, payment card data, or bank account information. Payment card data and bank account information are not stored in the system the company believes was affected.
>
> ***Yahoo is notifying potentially affected users and has taken steps to secure their accounts, including requiring users to change their passwords***. Yahoo has also invalidated unencrypted security questions and answers so that they cannot be used to access an account.
>
> * * *
>
> Yahoo encourages users to review all of their online accounts for suspicious activity and 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 using Yahoo Account Key, a simple authentication tool that eliminates the need to use a password on Yahoo altogether.

103. Commenting on the 2013 Data Breach, InfoArmor's Andrew Komarov said the Yahoo hack is different than other hacks: "The Yahoo hack makes cyber espionage extremely efficient . . . Personal information and contacts, e-mail messages, objects of interest, calendars and travel plans are key elements for intelligence-gathering in the right hands. The difference of the Yahoo hack between any other hack is in that it may really destroy your privacy, and potentially have already destroyed it several years ago without your knowledge."[43]

104. Many articles discussing the breach were published on the heels of the Company's public disclosure. The New York Times published an article titled "Yahoo Says 1 Billion User Accounts Were Hacked," which discussed how the disclosure of the 2013 Data Breach revealed Yahoo's lax security measures:

[43] *See* http://www.bloomberg.com/news/articles/2016-12 15/stolen-yahoo-data-includes-governmentemployee-information

> ***Security has taken a back seat at Yahoo in recent years, compared to Silicon Valley competitors like Google and Facebook. Yahoo's security team clashed with top executives, including the chief executive, Marissa Mayer, over the cost and customer inconvenience of proposed security measures***.
>
> And critics say the company was slow to adopt aggressive security measures, even after a breach of over 450,000 accounts in 2012 and series of spam attacks — a mass mailing of unwanted messages — the following year.
>
> "What's most troubling is that this occurred so long ago, in August 2013, and no one saw any indication of a breach occurring until law enforcement came forward," said Jay Kaplan, the chief executive of Synack, a security company. "Yahoo has a long way to go to catch up to these threats."[44]

105. The article also revealed that, in response to the discovery of the 2013 Data Breach, Yahoo is requiring "all of the affected users to change their passwords and it is invalidating unencrypted security questions — steps that it declined to take in September," when it announced the 2014 Data Breach.[45]

106. An article published on Time, Inc.'s Money magazine website further discussed the severity of the attack:

> ***Most alarming of all, the breaches may have put information related to national security at risk***. Bloomberg reported that upward of 150,000 U.S. government and military employees — including members of the FBI, CIA, White House, and others working with extremely sensitive information — are among those affected by the Yahoo 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.
>
> It's a leak that could allow foreign intelligence services to identify employees and hack their personal and work accounts, posing a threat to national security.

107. Analysts dubbed the 2013 Data Breach "***the Exxon Valdez of security breaches***," given the fact that "1 billion accounts [were] compromised, when there are only 3 billion people with Internet access in the world."[46]

---

[44] 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 .

[45] *Id*.

[46] 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 .

The 2014 Data Breach

108. In 2014, Russian-sponsored hackers stole the account information of some 500 million Yahoo users, including names, e-mail addresses, telephone numbers, dates of birth, passwords (created with MD5 algorithms), and security questions and answers ("2014 Data Breach" or "Siberia Intrusion"). Cybersecurity experts likened the 2014 Data Breach to an "ecological disaster." These hackers were able to traverse the Company's systems using Yahoo employee credentials to access Yahoo's user database (''UDB"), which contained usernames and passwords, as well as sensitive user information, such as users' names, email addresses, telephone numbers, dates of birth, and, in some cases, encrypted or unencrypted security questions and answers.

Criminal Indictment Reveals Details About the 2014 Data Breach

109. Details of the 2014 Data Breach are set forth in a March 2017 Indictment by the U.S. Justice Department (the "Indictment"). The Indictment charges two Russian intelligence agents and two hackers with masterminding the 2014 theft of 500 million Yahoo accounts, marking the first time the U.S. government criminally charged Russian spies for cyber offenses. The 47-count Indictment includes charges of conspiracy, computer fraud and abuse, economic espionage, theft of trade secrets, wire fraud, access device fraud and aggravated identity theft.

110. According to the Indictment, from at least in or about January 2014 up to and including at least in or about December 2016, officers of the Russian Federal Security Service ("FSB"), an intelligence and law enforcement agency of the Russian Federation ("Russia") headquartered in Lubyanka Square, Moscow, Russia, and a successor service to the Soviet Union's Committee of State Security ("KGB"), conspired together and with each other to protect, direct, facilitate, and pay criminal hackers to collect information through computer intrusions in the United States and elsewhere. The FSB officers, defendants Dmitry Dokuchaev, Igor Sushchin, and others known and unknown to the Grand Jury, directed the criminal hackers, defendants Alexsey Belan, Karim Baratov, and others known and unknown to the

Grand Jury (collectively, the "conspirators"), to gain unauthorized access to the computers of companies providing webmail and internet-related services located in the Northern District of California and elsewhere, to maintain unauthorized access to those computers, and to steal information from those computers, including information regarding, and communications of, the providers' users.

111. The Indictment states that in or around early 2014, the conspirators gained unauthorized access to Yahoo's network and began their reconnaissance. After gaining unauthorized access to Yahoo's network, Belan located and stole relevant Yahoo network resources of interest, including Yahoo's user database and its account management tools. Information stolen in the breach included names, email addresses, phone numbers, birth dates, encrypted password, and security questions and answers. The conspirators used their unauthorized access to Yahoo's network to identify and access accounts of, among other victims, users affiliated with U.S. online service providers, including but not limited to webmail providers and cloud computing companies, whose account contents could facilitate unauthorized access to other victim accounts; Russian journalists and politicians critical of the Russian government; Russian citizens and government officials; former officials from countries bordering Russia; and U.S. government officials, including cyber security, diplomatic, military, and White House personnel.

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

113. At the time of the 2014 Data Breach, Belan was one of FBI's Cyber Most Wanted criminals since 2012. An Interpol Red Notice seeking his immediate detention had been lodged

(including with Russia) since July 26, 2013. The FBI accused Belan of hacking into three major e-commerce companies between 2012 and 2013, stealing the user data and the encrypted passwords of millions of accounts and selling the information. Two separate federal arrest warrants and indictments for Belan have been issued in connection with those thefts. One was issued on September 12, 2012, in the U.S. District Court, District of Nevada, Las Vegas, after Belan was charged with obtaining information by computer from a protected computer; possession of fifteen or more unauthorized access devices; and aggravated identity theft. The second warrant was issued on June 6, 2013, in the U.S. District Court, Northern District of California, San Francisco, after Belan was charged with two counts of fraud in connection with a computer and two counts of aggravated identity theft.[47]

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

115. The Criminal Indictment confirms precisely what the Company knew since at least December 2014 and early 2015 at the latest — *i.e.*, that state-sponsored actors from Russia had hacked into Yahoo's network, stolen substantial amounts of Yahoo user information, and used that stolen information to gain unauthorized access to Yahoo user accounts.

116. More specifically, according to the Criminal Indictment, in 2014, the four criminal defendants gained unauthorized access to user information for 500 million Yahoo user accounts — *i.e.*, the Siberia Intrusion. Specifically, the criminal defendants stole user information held in the Company's UDB, including account users' names; recovery e-mail accounts and phone numbers; password verification questions and answers; and certain cryptographic security information associated with the

[47] *See* https://www.fbi.gov/wanted/cyber/alexsey-belan

account, *i.e.*, the account's "nonce." The UDB is accessible by using the account management tool ("AMT"), a cryptographic key that deciphers the encrypted information in the UDB.

117. Not only did the criminal defendants gain access to a wide array of Yahoo user information in the UDB, they also used their access to the AMT to maintain persistent unauthorized access to compromised accounts. By combining the UDB and access to the AMT, the criminal defendants were able to gain access to and search within Yahoo user accounts. The Criminal Indictment alleges that the criminal defendants' conduct "was part of a larger intrusion into Yahoo's computer network, ***which continued to and including at least September 2016***. As part of this intrusion, malicious files and software tools were downloaded onto Yahoo's computer network, and used to gain and maintain further unauthorized access to Yahoo's network." These facts undermine Yahoo's frequent statements, as part of Defendants' attempted cover-up, that Yahoo had successfully eradicated the hackers from Yahoo's networks by early 2015 and that Defendants were allegedly unaware of the data exfiltration.

118. The Company now admits that the information security team, senior executives, and legal staff, who reported directly to the Board or sat on the Board (which included Defendant Mayer), knew that state-sponsored hackers had access to the Company's AMT as early as late 2014. In the 2016 Form 10-K, the Company admitted that "[i]n late 2014, senior executives and relevant legal staff were aware that a state-sponsored actor had accessed certain user accounts by exploiting the Company's account management tool."

119. Moreover, Yahoo now admits that the information security team understood that these state-sponsored actors had exfiltrated copies of the Company's UDB files containing the personal data of Yahoo users.

120. The Criminal Indictment also alleges that the criminal defendants accessed Yahoo user account information and contents by both internally and externally minting authentication cookies. By

minting cookies, the criminal defendants gained access to Yahoo's network or the associated Yahoo accounts without the need to enter a username and password.

121. With respect to the external minting of cookies, the criminal defendants used the "nonce" associated with individual Yahoo user accounts stored in the UDB, which was stolen in 2014. As the Criminal Indictment makes clear, however, the criminal defendants could have been deterred from doing so if Yahoo had notified users and had them change their passwords. This is because whenever a Yahoo user changed his or her password, the nonce associated with the account changed as well. Because the Company failed to notify users of the Siberia Intrusion, Yahoo users did not change their passwords, and thus the criminal defendants were able to utilize the nonce associated with user accounts for a period of two years.

122. The compromised accounts would have affected more than just e-mail. Breaking into a Yahoo account would give the hackers access to users' activity on Flickr, Tumblr, fantasy sports, and other Yahoo applications. *See* Ellen Nakashima, "Justice Department Charges Russian Spies and Criminal Hackers in Yahoo Intrusion," THE WASHINGTON POST (Mar. 15, 2017). In the 2014 hack, the FSB — Russia's Federal Security Service, and a successor to the KGB — sought the information for intelligence purposes, targeting journalists, dissidents, and U.S. government officials, but allowed the criminal hackers to use the e-mail cache for the officials' and the hackers' financial gain, through spamming and other operations.

Defendants Had Contemporaneous Knowledge of the 2014 Data Breach and of Prior Breaches

123. Because of the importance to Yahoo's operations and financial results of cybersecurity and compliance with applicable laws, the Board (including Defendant Mayer) and the Audit and Finance Committee of the Board ("AFC") received detailed updates from management about the Company's cybersecurity, including information about any data breaches.

124. The Board and the AFC also received consistent updates on a quarterly basis from Yahoo's CISO. These updates included a review of data security breaches, both large and small.

125. During the Class Period, the AFC received updates from the CISO 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.

126. The AFC's Charter states that it is responsible for briefing the Board on important matters: "The 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."

127. Moreover, the Board received updates from the CISO at a minimum of 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. According to the deposition testimony of Thomas McInerney—who was a member of Yahoo's Board and AFC from 2012 up to the Verizon Transaction and is currently the president and CEO of Altaba—during the CISO presentations, the Board received updates on protecting the Company's electronic assets, websites, communications, incident responses, and breaches and hacks of the Company's systems.

128. For years, as noted, the refusal of Yahoo's Board and senior management to devote the necessary resources to adequately remediate the known deficiencies in the Company's data security infrastructure exposed the Company to significant hacking incidents.

129. The Board and management had knowledge of repeated red flags putting them on notice that the Company's data security infrastructure was inadequate. In fact, one of the documents reviewed by the AFC in 2016 was entitled "Alex - Marissa Presentation," a presentation most likely presented to

Defendant Mayer in or around 2013. The document identified four hacking incidents known to the Company from 2008 through 2013, which were summarized as follows:

a. November 2008: Intruders attack Yahoo's systems, compromising at least 46 employee credentials that allowed them to compromise the account management tool. This hacking incident resulted in 70 systems being infected, with the attackers establishing permanent VPN access to the corporate network.

b. July 2009: Intruders attack Yahoo's systems with the objective of gaining access to the AMT.

c. February 2012: Intruders levy a second attack on Yahoo's data security infrastructure and successfully infect 85 systems.

d. February 2013: Intruders wage a third attack on Yahoo's data security infrastructure with the objective of gaining access to the account management tool. The intruders successfully infect 28 systems within Yahoo's internal systems.

130. From the outset, Yahoo was well-aware that Russian hackers had compromised the Company's internal systems and had stolen millions of Yahoo user credentials. The information security team was meticulous in investigating and documenting the breach, which was internally assigned the code name "Siberia Intrusion." Specifically, the information security team not only conducted its own internal investigation, but a third-party forensic expert was also hired in 2014 to confirm the findings of the internal investigation.

131. The first signs inside Yahoo of the Siberia Intrusion came at least as early as about October 9, 2014, when the Company's information security team (internally denigrated as the Paranoids) detected the presence of the Russian hackers in the Company's systems. From that point until at least February

2015, the Paranoids tracked the movements of the Russian hackers as they made their way throughout Yahoo's internal systems.

132. By November 2014, Yahoo— including key members of its legal team— knew about the 2014 Breach. In email exchange on or about November 5, 2014, a Yahoo Software Development Engineer and a member of Yahoo's "Incident Response" team discussed a meeting with the legal team about the 2014 Breach, referring to the breach as "Siberia shit":

11.5.14, 11:06	Andrew R.	Hey Jeff, are you guys still having the strategy meeting?
11.5.14, 11:10	Jeff Z.	ah sorry, Ramses [Martinez] is caught up with Legal. Ill ping you if he gets finished.
11.5.14, 11:10	Jeff Z.	Siberia shit……

133. At about the same time, Yahoo's decision-makers made a conscious and deliberate decision not to alert any of Yahoo's customers that their "Personal Identifying Information" ("PII") had been stolen or compromised and also created (but never used) a "reaction" press release to be employed in the event the breach was leaked to the public.

134. While the hacking was on-going, Yahoo held a large number of high level meetings to discuss and analyze the Siberia Intrusion. The information security team held daily meetings—sometimes more than one per day—for a period of several months. The legal team, including Defendant Bell, attended most of the information security meetings. Moreover, while the information security team was responding in real time to the Siberia Intrusion, Yahoo co-founder David Filo—a substantial shareholder who owned about 7.4% of Yahoo's outstanding shares and served as a member of the Board from June 2014—was present in the Paranoids' war room, and thus privy to the investigation and its findings.

135. In addition to daily and weekly meetings, the Paranoids documented their findings and conclusions for the Siberia Intrusion. According to Stamos, the Company's CISO at the time, the information security team generated numerous forensic analyses that were used to report the findings and conclusions to members of management and the Board, including: (1) forensic reports dedicated to specific servers; (2) a master narrative that tied all forensic reports together; and (3) a very large chart that the information security team kept updated showing the data flow between all the different machines as well as to external servers. Stamos testified under oath that he brought the very large chart to one of the AFC meetings, although he could not recall which one, in order to brief the AFC members on the scope and impact of the Siberia Intrusion.

136. Martinez, Senior Director of the Paranoids, also testified under oath that Yahoo created multiple detailed reports for the Siberia Intrusion, including: (1) lengthy and detailed Incident Reports; (2) an Incident Presentation; and (3) a presentation presented to the AFC at the June 23, 2015 meeting. These reports included a description and chronology of events, results of the analysis, a chart reflecting exfiltration of the data and movement of the stolen information from computer to computer, and conclusions reached. The information security team used the Incident Reports and other data to prepare summaries provided to management and the Board, which they called Incident Presentations.

137. The information security team members all agreed that the Siberia Intrusion represented a significant security breach requiring a quick and aggressive response.

138. After it was detected by the Yahoo information security team, the hacking activity began to increase significantly.

139. In response, on November 14, 2014, Yahoo engaged Dell SecureWorks, a third-party forensic expert, to aid with its investigation. As a result of a three-month forensic investigation, Dell

issued a report to Martinez on February 2, 2015, entitled, "Incident Response and Forensics Letter Opinion" (the "Dell SecureWorks Report"), which summarized the Siberia Intrusion.

140. Like the Company's internal investigation, the Dell SecureWorks Report concluded that "incident responders identified a large-scale intrusion during Q420l4 in which the intruders targeted Linux and BSD systems across a broad spectrum of Yahoo's production and corporate networks." Importantly, the Dell SecureWorks Report also concluded that the intruders had, in fact, exfiltrated data from Yahoo's systems: "the intruders eventually gathered user credentials for internal networks as well as VPN tokens for entering the network from the outside . . . [T]he primary targets of the Siberia intrusion appeared to be end-user data and information that would aid in maintaining access to that data."

141. No disclosure was made to affected Yahoo users or to investors.

142. The findings from the internal investigation, confirmed by Dell, were summarized by Martinez in an Incident Presentation created some time after December 2014. The Incident Presentation contained all material facts related to the Siberia Intrusion. For instance, the Presentation contained a detailed chronology relating to the Company's knowledge of the attack, which included the following information:

- 9/8/14: Intrusion starts
- 10/9/14: Intrusion detected by Paranoids
- 11/4/14: Compromised employee credentials used to log in to UDB hosts
- 11/4/14: Attackers find UDB weekly backup files
- 11/9/14: Attackers move backup files to [location redacted]
- 11/10/14: UDB backup files are transferred via FTP to a host in the Russian Federation
- 11/10/14: Attackers delete UDB backup files

- 12/8/14: Deleted files are found and recovered by Paranoids

143. The Incident Presentation made it clear that the Russian hackers had in fact exfiltrated Yahoo user data, including usernames and passwords. To illustrate the exfiltration, the Incident Presentation contained exfiltration charts and examples identifying the flow of information.

144. As Martinez testified, data exfiltration was discussed early and often with everyone in the reporting chain, including senior management and the Board.

145. The Company not only knew that data had been stolen, but also put an estimate on the number of compromised accounts that even non-experts would have found to be significant. In a slide entitled "Impact Analysis," the Incident Presentation summarized the conclusions of the Siberia Intrusion investigation. The Incident Presentation described the Siberia Intrusion as a "[s]tate sponsored attack" carried out by "Russia based actors" who "[t]argeted access via [the account management tool] to user and Yahoo executive accounts." With regard to the data compromised, the Incident Presentation noted that the "[***best case scenario" was that "108M [million] credentials in UDB" were "compromised." The "[w]orst case scenario" was that "[a]ll credentials in UDB" were "compromised***."

146. Thus, based on the Company's thorough investigation, the information security team was well aware that the Company had experienced a catastrophic hacking incident affecting potentially all Yahoo user credentials. This information was routinely and comprehensively presented to Yahoo's management and the Board, as discussed below, but hidden from investors.

The Information Security Team Notified Senior Management of All Relevant Details Regarding the Siberia Intrusion

147. As aforementioned, the information security team had extensive contemporaneous knowledge about the Siberia Intrusion. The information security team provided numerous updates to management and the Board about the Siberia Intrusion.

148. Both Stamos and Martinez testified that they reported all material facts about the Siberia Intrusion to management, and that there was ample knowledge within the Company of everything that was happening, the impact on the Company's systems and Yahoo user data, and what needed to be done in response.

149. Specific meetings with management were a norm during the time period from October 2014 to December 2014. Stamos met with senior management, including Mayer and Filo, on at least four or five occasions to specifically discuss the Siberia Intrusion. In addition, Stamos provided extensive additional reporting on the Siberia Intrusion to SVP Jay Rossiter and Defendant Bell, who were simultaneously attending weekly meetings with Mayer.

150. During these meetings, Stamos communicated everything the information security team knew about the Siberia Intrusion to management, including the findings and conclusions contained in the Incident Presentation (discussed above). Stamos testified that the information security team was not the only department that knew that the Russian-sponsored hackers infiltrated Yahoo. Martinez similarly noted in deposition that data exfiltration reports were widely disseminated throughout the Company, including to upper management.

151. Stamos testified that Mayer, Bell, and Filo had contemporaneous knowledge of the Siberia Intrusion, including the fact that a massive number of Yahoo accounts had been compromised.

The Board Received Repeated Updates Regarding the Siberia Intrusion

152. As noted above, the Board and the AFC routinely received updates regarding data breaches into the Company's systems. This was also true for the Siberia Intrusion. At least during the employment of Stamos and Martinez (both of whom left the Company before 2016), the AFC received numerous briefings on the Siberia Intrusion. The Board materials from October 15, 2014, April 15, 2015, and June 23, 2015 show that detailed information about the Siberia Intrusion was provided to the AFC. During those briefings, neither Stamos nor Martinez concealed any information from the AFC and, in

fact, testified that they told the Board everything they knew. This included all information uncovered during the internal investigation, as well as the information which was subsequently confirmed in the Dell Secure Works Report.

153. Defendants went to great lengths to conceal the existence of the breach. The Board's and the AFC's meeting materials reflect 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.*, "Corporate Intrusion History" and "Nation State Update").

154. The intentional vagueness in the written Board and committee materials was confirmed by Martinez at his deposition. He testified that the legal department told him to keep details of his presentations to the Board about security incidents out of any written materials presented to the Board. This instruction was given to avoid creating a paper trail, as the legal department told Martinez only to convey detailed information about security incidents ***orally***.

155. On April 15, 2015, the AFC discussed, among other things, the CISO update, given by Stamos, including "the information security risks for the Company in 2015 and measures being taken to analyze as well as combat those risks." The AFC materials contain a section entitled "Security Review and 2015 Priorities," which had been "PREPARED AT THE REQUEST OF THE GENERAL COUNSEL."

156. The April 15, 2015 AFC materials innocuously refer to "Yahoo!'s Year in Review," without any description of the Siberia Intrusion.

157. Although the committee materials contain non-descriptive slides, Stamos testified that he reported all material facts relating to the Siberia Intrusion to the AFC, including all information uncovered during the Company's internal investigation and confirmed by Dell Secure Works. Critically, no disclosure was made to affected Yahoo users at the time, or to investors.

158. Moreover, all information presented to the AFC must be presumed to have subsequently been conveyed to the entire Board. According to the AFC's 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[.]"

159. 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." Consistent with these responsibilities, the AFC must be presumed to have reported to the Board the details of the Siberia Intrusion as reported to them by Stamos.

160. On June 23, 2015, Martinez attended a meeting of Yahoo's AFC, which was also attended by McInerney and Defendants Mayer, Stamos and Bell, and SVP Jay Rossiter. Although Stamos, then-CISO, was in attendance, Martinez conducted the CISO update to the AFC. He informed the Committee about the details of the Siberia Intrusion.

161. In a section of the June 2015 presentation entitled "Paranoid Strategy and Roadmap," Martinez provided the AFC members with a detailed presentation regarding the Siberia Intrusion, as reflected by a slide entitled "Nation State Update." The fact that Martinez presented the details of the Siberia Intrusion directly to the AFC is consistent with the scope and gravity of the attack, which as the Dell Secure Works Report stated was "large-scale," "across a broad spectrum of Yahoo's production and corporate networks," and exposed Yahoo users to ongoing exploitation of personal information. Consistent with its significance to the Company, and as the recipient of the Dell Secure Works Report, Martinez disclosed to the AFC every relevant fact relating to the Siberia Intrusion during the "Nation

State Update" at the June 23, 2015 AFC meeting, including the existence of data exfiltration. Again, however, no disclosure was made to affected Yahoo users or to investors.

162. Consistent with the responsibilities outlined in the AFC charter and Yahoo's Corporate Governance Guidelines discussed above, the AFC must be presumed to have reported to the Board the details of the Siberia Intrusion as reported to them by Martinez.

163. Throughout the 2015 and 2016 period, Yahoo implemented certain security measures in response to the Siberia Intrusion, some of which had been recommended in the Dell Secure Works Report.[48] The Board received repeated updates about the security measures implemented in response to the Siberia Intrusion at each meeting held during this time:

a. On October 14, 2015, the AFC discussed the security measures taken in response to the Siberia Intrusion, including the search for a new CISO, the Company's overall security status in 2015, the Company's achievements in the past year, the key priorities going forward, and the Company's plans to conduct an external assessment of the strengths and weaknesses of the Company's security measures.

b. On December 2, 2015, the AFC reviewed a report written by Rapid7, a third party cybersecurity expert, concerning its cybersecurity assessment. Rapid7 noted that it had been conducting interviews with the Paranoids, Legal, and tech teams, as well as received documentation regarding the Company's processes and standards for security incidents.

c. On February 22, 2016, the AFC received an update from Bob Lord, the Company's new CISO, discussing Rapid7's cybersecurity assessment. The update included a review of the areas reviewed by Rapid7 as part of the assessment, the results of the assessment,

[48] In its Form 10-K, filed on March 1, 2017, the Company admits that "significant additional security measures were implemented in response to" "the 2014 compromise of user accounts, as well as incidents by the same attacker involving cookie forging in 2015 and 2016."

comparison to peers, critical recommendations and a remediation plan. The cybersecurity assessment showed that the Company ranked very low in its ability to identify, protect, and detect data security intrusions. This information was concealed from investors.

d. April 13-14, 2016 Board meeting materials indicate that the Board once again discussed the security incidents at the Company over the past 24 months and remedial efforts being taken to shore up the Company's data security infrastructure.

Yahoo Continued Concealing the Breaches While It Shopped for a Suitor

164. Yahoo management had knowledge of the Siberia Intrusion and of other breaches, yet affirmatively decided not to disclose them.

165. The Board was complicit in the decision not to disclose the Siberia Intrusion for nearly two years. As set forth above, the AFC and Board had knowledge of the Siberia Intrusion, its effects (including data exfiltration), and the risks to Yahoo.

166. Still, the Board and management continued to withhold this material information to achieve the goal of selling off Yahoo's flailing operating assets.[49]

167. In July 2016, facing intense pressure from stockholders, and desperate to consummate the Verizon Transaction, the Board (including Defendant Mayer) made affirmative misrepresentations to Verizon and to investors, which were known by Yahoo to be false at the time they were made.

168. Notwithstanding the fact that the Board had knowledge of the Siberia Intrusion, for example, at a July 22, 2016 Board meeting, the Board reviewed and approved provisions in the SPA 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. Yahoo's

[49] In or about January 2016, Yahoo's Board formed a "Strategic Review Committee" composed of outside directors (including Thomas McInerney, who had served on the AFC in 2014 and 2015) to work with Yahoo's financial advisors who, beginning in February and throughout the spring of 2016, solicited proposals from interested bidders. SEC Form DEF 14A, filed April 24, 2017, at 40-41, 53.

assurances that it experienced no security breaches or theft were made in public filings published with the SEC for investors' review.[50]

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

170. In late July 2016, Verizon privately raised with Company management concerns that Yahoo user data had been compromised, after Verizon Chairman and CEO Lowell McAdam received an email from a hacker who claimed to have obtained the personal information of 280 million Yahoo users and provided a 5,000-record sample file. This chain of events was described in a subsequently prepared AFC document entitled "Talking Points for Calls with Verizon."

171. Joseph Cox, a reporter with the technology news site Motherboard, said he emailed Yahoo on July 30, 2016, to ask if the Company was aware that Peace was attempting to sell Yahoo data. In a response email to Motherboard, a Yahoo spokesperson said "***We are aware of a claim*** . . . We are committed to protecting the security of our users' information and we take any such claim very seriously. Our security team is working to determine the facts. Yahoo works hard to keep our users safe, and we always encourage our users to create strong passwords, or give up passwords altogether by using Yahoo Account Key, and use different passwords for different platforms." Yahoo provided no other details and

[50] The SPA defined a "Security Breach" as "any actual (i) loss or misuse (by any means) of Personal Data; (ii) unauthorized or unlawful Processing, sale, or rental of Personal Data; or (iii) other act or omission that compromises the security or confidentiality of Personal Data."

declined to say if the claim exposing a breach was legitimate. [51]

172. According to reports, Yahoo's awareness of "Peace's" claim extended to the Company's CEO, defendant Mayer.[52]

173. Peace told Motherboard, "well f*** them they dont want to confirm well better for me they dont do password reset."[53]

174. Even at this point, however, the Company delayed disclosing the Siberia Intrusion until September 22, 2016, in an effort 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, "[r]umors 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."

175. As rumors of a massive breach continued to percolate in the market, the Board and AFC met several times to discuss the Siberian Intrusion.

176. On September 13, 2016, more than a week before the Company finally publicly acknowledged that Yahoo suffered one of the most significant data breaches in history, Yahoo's Board held a special meeting to "receive an update on and to discuss the Company's investigation into the data security incident involving the potential exfiltration of data by what the Company believed to be a state-sponsored actor in late 2014."

177. Two days later, on September 15, 2016, the AFC was provided via secure download a packet of materials compiling what it knew about the Siberia Intrusion before the Verizon Transaction.

---

[51] Joseph Cox, *Yahoo "Aware" Hacker is Advertising 200 Million Supposed Accounts on Dark Web*, Motherboard, Aug. 1, 2016.

[52] 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 .

[53] Joseph Cox, *Yahoo "Aware" Hacker is Advertising 200 Million Supposed Accounts on Dark Web*, Motherboard, Aug. 1, 2016.

178. The package of materials included, *inter alia*, a document entitled "Users to Be Notified;" the October 2014 presentation that disclosed "[s]everal major incidents;" a copy of the Dell Secure Works Report; the CISO update for the April 15, 2015 AFC meeting; AFC Minutes for the April 15, 2015 AFC meeting; the CISO update for the June 23, 2015 AFC meeting, where Martinez provided the AFC with a "Nation State Update" relating to the findings of the Dell SecureWorks Report; AFC Minutes for the June 23, 2015 AFC meeting; a package on messaging, including draft notifications to users regarding the Siberia Intrusion, and the above-mentioned talking points memorandum for Verizon negotiations.

179. On September 15, 2016, AFC also reviewed the "RISK FACTORS ON SECURITY" set forth in Yahoo's second quarter 2016 Form 10-Q.

180. Two days later, on September 17, 2016, the Board met again to discuss the Siberia Intrusion. The Board's minutes report, *inter alia*, that Bob Lord, the current CISO, discussed "the process used by the state-sponsored actor to impersonate users, how cookies were forged and used to log in the system, and how the Company was able to detect the state-sponsored actor." Despite Defendants' awareness that that the Russian hackers had minted forged cookies for Yahoo user accounts, Yahoo omitted disclosure of this information until November 2016.[54]

181. On September 17, 2016, according to the minutes, the Board discussed a *new* "proposed investigation process and authorized the AFC to investigate the 2014 Data Security Incident." In that regard, Defendant Mayer drew the Board's attention to materials, distributed to the Board in advance of the meeting, "pertaining to the Company's investigation into the data security incident involving the potential exfiltration of data by what the Company believed to be a state-sponsored actor in late 2014." The "proposed investigation process" concerning the Siberia Intrusion would include at least one AFC

[54] Yahoo eventually disclosed the Forged Cookie Breach on November 9, 2016, burying it in two short references in a 141-page Form 10-Q.

member, outside Director Thomas McInerney, who had received the CISO updates given to the AFC from October 2014 to October 2015 regarding the Siberia Intrusion.

182. Only subsequently did the Board conclude that McInerney should no longer oversee the 2016 investigation into the Siberia Intrusion given the fact that he was on the AFC in 2015 but did allow McInerney (who at about this time was being offered the top position at Yahoo's successor company) to continue to lead the Strategic Review Committee—a role that allowed him to renegotiate a release for himself and others relating to claims held by Verizon as a result of the breach of the SPA.

183. On September 19 and 21, 2016, the Board held telephonic meetings to discuss the investigation into the Siberia Intrusion.

184. On September 22, 2016, the AFC received and reviewed a package of materials similar to the materials that were provided to the AFC on September 15, 2016. The AFC also reviewed the Incident Presentation created by Martinez in or around 2015, which formed the basis for the updates provided to the AFC and management in 2015.

In a Misleading Press Release, Yahoo Finally Discloses the Breach

185. Finally, on September 22, 2016, Yahoo disclosed that data associated with 500 million users' accounts was stolen. Only at that time, Yahoo told users to change their password and security questions and review their accounts for suspicious activity:

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

> Yahoo is notifying potentially affected users and has taken steps to secure their accounts. These steps include invalidating unencrypted security questions and answers so that they cannot be used to access an account and asking potentially affected users to change their passwords. Yahoo is also recommending that users who haven't changed their passwords since 2014 do so.
>
> Yahoo encourages users to review their online accounts for suspicious activity and to change their password 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 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.

186. The press release was false and misleading because it failed to disclose that Defendants had concurrent knowledge about the breaches. For example, it was misleading to suggest that the data exfiltration was only discovered through a "recent" investigation, when in fact Yahoo conducted an investigation in 2014 and 2015 and hired Dell in 2014 to perform a forensic investigation, which concluded at that time that at least 108 million and potentially all of Yahoo's user credentials had been compromised.

187. The above press release was also filed with the SEC on September 22, 2016 as an exhibit to a Form 8-K disclosure, which was false and misleading because, among other things, it represented that Yahoo's investigation was "recent."

188. Moreover, the September 22, 2016 Press Release falsely represented that the stolen account information "*may have* included names, email addresses, telephone numbers, dates of birth, hashed passwords (the vast majority with bcrypt) and, in some cases, encrypted or unencrypted security questions and answers." This representation was materially misleading because the 2014 Dell SecureWorks Report explicitly stated that this exact information had in fact been stolen.

189. Finally, the September 22, 2016 Press Release failed to disclose that the Company knew that the Russian hackers had been minting cookies—a fact the Board had learned or revisited during the September 17, 2016 meeting, as set forth above.

190. On September 27, 2016, the Board convened a further special telephonic meeting to discuss the "the AFC's ongoing investigation," "the oversight and management process," and recent press coverage. Defendant Mayer provided "background and additional information," including "background the Board had previously discussed at prior Board meetings." Following a discussion, the Board approved the formation of a special committee to conduct "the sole and exclusive independent investigation on behalf of the Board" of the Siberia Intrusion (the "Independent Committee"), which now excluded McInerney, as noted above, and which would engage Sidley Austin LLP as "independent legal counsel."

191. As the Company later averred, the so-called Independent Committee's task was purportedly to investigate the "scope of knowledge within the Company in 2014 of access to Yahoo's network by the state-sponsored actor responsible for the theft and related incidents, and Yahoo's internal and external reporting processes and remediation efforts related to the 2014 Security Incident and related incidents." April 24, 2017 SEC Form DEF 14A, at 56.

192. Despite the explicit concern with independence, throughout the fall of 2016, the Board permitted Defendants Mayer and Bell to play a substantial role in a parallel internal investigation, including providing information to the Independent Committee, the Board, and the Strategic Review Committee (still headed by McInerney and also including the two members of the Independent Committee) about the Siberia Intrusion and fully participating in Board and Board committee meetings discussing the Siberia Intrusion and its effect on the Verizon transaction.

193. Also during the fall of 2016, Strategic Review Committee head McInerney was holding discussions about becoming the CEO of Yahoo's successor once the Verizon transaction was completed and was provided with a draft employment agreement—months before the Independent Committee (from which he had been recused) had completed its investigation.

194. Yahoo was lambasted for taking at least two months to report the breach to the public. Senator Richard Blumenthal stated that '"[i]f Yahoo knew about the hack as early as August [2016], and failed to coordinate with law enforcement, taking this long to confirm the breach is a blatant betrayal of their users' trust.'"[55] Senator Blumenthal called on law enforcement and regulators to '"investigate whether Yahoo may have concealed its knowledge of this breach in order to artificially bolster its valuation in its pending acquisition by Verizon.'"

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

196. The 2014 Data Breach shares similarities to the 2013 hack. Indeed, in a February 23, 2017 letter to John Thune, Senate Chairman of the Committee on Commerce, Science and Transportation and Jerry Moran, Senate Chairman of the Subcommittee on Consumer Protection, Product Safety, Insurance and Data Security, Yahoo stated that "[a] majority of the user accounts that were potentially affected by the 2014 Incident are also believed to have been affected by the 2013 Incident."[56]

---

[55] Seth Fiegerman, *Yahoo Says 500 Million Accounts Stolen*, CNN Tech (Sept. 23, 2016), http://money.cnn.com/2016/09/22/technology/yahoo-data-breach .

[56] 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 .

The Forged Cookie Data Breach

197. On March 1, 2017, the Company began notifying approximately 32 million Yahoo users that they had been the victim of yet another breach, this time a "forged cookie" data breach in 2015-2016 (the "Forged Cookie Breach"). "Based on the investigation, we believe an unauthorised third party accessed the company's proprietary code to learn how to forge certain cookies," the Company said. "Forged cookies could allow an intruder to access users' accounts without a password," Yahoo explained. The Company has connected some of this activity to the same state-sponsored actor believed to be responsible for the 2014 Data Breach.

198. The forged cookie data breach was related to the 2014 Data Breach and facilitated by the data stolen in the 2014 Data Breach.

199. Defendants' failure to disclose the 2013 and 2014 Data Breaches, as well as their failure to adequately improve Yahoo's data security after numerous breaches, including the 2013 and 2014 Data Breaches, directly allowed hackers to continue to infiltrate Yahoo's databases in 2015 and 2016.

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

201. Yahoo said that it has forced password resets and invalidated the forged cookies.

Additional Allegations Demonstrating Defendants' Contemporaneous Knowledge of the Breaches

202. As set forth above, Defendants failed to notify investors about the 2013 Data Breach, the 2014 Data Breach, and the Forged Cookie Data Breach for years, despite their contemporaneous knowledge of the hacks.

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

> In late July 2016, a hacker claimed to have obtained certain Yahoo user data. After investigating this claim with the assistance of an outside forensic expert, the Company could not substantiate the hacker's claim. Following this investigation, the Company intensified an ongoing broader review of the Company's network and data security, including a review of ***prior access to the Company's network by a state-sponsored actor that the Company had identified in late 2014***. Based on further investigation with an outside forensic expert, ***the Company disclosed the Security Incident on September 22, 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.
>
> As described above, the Company had identified that a state-sponsored actor had access to the Company's network in late 2014. An Independent Committee of the Board, advised by independent counsel and a forensic expert, is investigating, among other things, the scope of knowledge within the Company in 2014 and thereafter regarding this access, the Security Incident, the extent to which certain users' account information had been accessed, the Company's security measures, and related incidents and issues.
>
> In addition, the forensic experts are currently investigating certain evidence and activity that indicates an intruder, believed to be the same state-sponsored actor responsible for the Security Incident, created cookies that could have enabled such intruder to bypass the need for a password to access certain users' accounts or account information.

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

> As previously disclosed, an independent committee (the "Independent Committee") of the Board of Directors (the "Board") has investigated the Security Incidents[57] and related matters, including the scope of knowledge within the Company in 2014 of access to Yahoo's network by the state-sponsored actor responsible for the theft and related incidents, the Company's internal and external reporting processes and remediation efforts related to the 2014 Security Incident and related incidents. The Independent Committee has concluded its investigation, although it will continue to review developments

[57] The Security Incidents consist of the 2013 Data Breach, the 2014 Data Breach, and the Forged Cookie Data Breach.

regarding the Security Incidents and report to the Board on these issues, and cooperate with various government entities . . . .

Based on its investigation, the Independent Committee concluded that ***the Company's information security team had contemporaneous knowledge of the 2014 compromise of user accounts, as well as incidents by the same attacker involving cookie forging in 2015 and 2016. In late 2014, senior executives and relevant legal staff were aware that a state-sponsored actor had accessed certain user accounts by exploiting the Company's account management tool***. The Company took certain remedial actions, notifying 26 specifically targeted users and consulting with law enforcement. While significant additional security measures were implemented in response to those incidents, it appears certain senior executives did not properly comprehend or investigate, and therefore failed to act sufficiently upon, the full extent of knowledge known internally by the Company's information security team. Specifically, as of December 2014, the information security team understood that the attacker had exfiltrated copies of user database backup files containing the personal data of Yahoo users but it is unclear whether and to what extent such evidence of exfiltration was effectively communicated and understood outside the information security team . . .

* * *

Actions the Company is Taking in Response to the Independent Committee's Findings
Based on the Independent Committee's findings, the Board has taken the management related actions described below, adopted certain process and structure changes to address the Company's issues with respect to the Security Incidents, and taken certain other disciplinary actions.

Management Changes

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

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

Other Remedial Actions

Additionally, in response to the Independent Committee's findings and recommendations, the Board has directed the Company to implement or enhance a number of corrective actions, including revision of its technical and legal information security incident response protocols to help ensure: escalation of cybersecurity incidents to senior executives and the Board of Directors; rigorous investigation of cybersecurity incidents and engagement of forensic experts as appropriate; rigorous assessment of and documenting any legal reporting obligations and engagement of outside counsel as appropriate; comprehensive risk assessments with respect to cybersecurity events; effective cross-functional communication regarding cybersecurity events; appropriate and timely disclosure of

> material cybersecurity incidents; and enhanced training and oversight to help ensure processes are followed.

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

> Early this week I spoke with Marissa Mayer and expressed my appreciation for Yahoo's cooperation in this matter. This was not our first conversation. Ms. Mayer has demonstrated great leadership and courage while under intense pressure from many entities. ***She and her team at Yahoo have always been professional, engaged and responsive to our requests. They were great partners to be with during this two year investigation.*** This case illustrates that the FBI can work with victims, including those right here in Silicon Valley to address malicious cyber activities while respecting victim's sensitivities.

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

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

208. Reportedly, the British intelligence agency MI5 was brought in to help the U.S. probe as the actions of Russia's intelligence agency were classified as "hostile actors."

209. The hackers maintained their access to Yahoo's networks until at least October 2016, the FBI said.

210. Confidential witnesses with relevant knowledge, who were in a position to know the facts, also attest that Defendants knew about the 2013 and 2014 breaches from the start. These witnesses

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

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

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

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

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

214. Yahoo's own former executives reacted with disbelief at placing blame solely on Bell. Yahoo's former head of media, Scott Moore, called the condemnation "***ridiculous***," saying "I know @ronsbell_tech who is a good man and ***as a lawyer he wasn't in charge of security*** @Yahoo @lame CYA move @marrisamayer twitter.com/karaswisher/st…"

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

216. Even more troubling—and emblematic of Yahoo's continued intent to deceive—is its false representation in a September 9, 2016 regulatory filing with the SEC that "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 Yahoo's possession.

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

218. Yahoo saw its shares plunge immediately after each breach disclosure.

Yahoo Is Assailed for Failure to Fulfill Its Disclosure Obligations

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

220. According to the Ponemon Institute, which tracks data breaches, the average time it takes organizations to identify a data breach is 191 days after the date of the breach, and the average time to contain a breach is 58 days after its discovery.[58]

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

222. Yahoo's improprieties were quick to attract the ire of U.S. senators. Senator Mark Warner of Virginia was quoted stating that "[t]his most recent revelation [about the 2013 Data Breach] ***warrants a separate follow-up*** and I plan to press the company on why its cyber defenses have been so weak as to have compromised over a billion users."[59] Warner, the top Democrat on the Senate Intelligence Committee, described the hacks as "***deeply troubling*** . . . If a breach occurs, consumers should not be

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

[59] *See* http://www.fortune.com/2016/12/15/yahoo-hacksenator .

first learning of it three years later . . . Prompt notification enables users to potentially limit the harm of a breach of this kind, particularly when it may have exposed authentication information such as security question answers they may have used on other sites." Senator Warner said that "***Yahoo had a responsibility to be more forthcoming in publicly reporting this breach sooner than it did*** . . ."

223. On September 26, 2016, Senator Warner wrote a letter to the chair of the SEC urging the agency to evaluate whether Yahoo "fulfilled obligations to keep public and investors informed, as required by federal law":

> I write to you about important federal securities matters pertaining to the Yahoo breach that may have affected 500 million accounts, and the associated lack of disclosure by the company to the public.
>
> Last week, it was reported that Yahoo suffered a major breach in 2014, compromising more than 500 million accounts. Press reports indicate Yahoo's CEO, Marissa Mayer, knew of the breach as early as July of this year. ***Despite the historic scale of the breach, however, the company failed to file a Form 8-K disclosing the breach to the public***.
>
> Furthermore, Yahoo has been engaged in an effort to sell its Internet business, including the unit affected by the breach, to Verizon since at least July 25, 2016, yet Yahoo reportedly did not inform Verizon of the breach until September 20, 2016. More puzzlingly, the company noted in a proxy statement as recently as September 9, 2016 that, "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."
>
> Disclosure is the foundation of federal securities laws, and public companies are required to disclose material events that shareholders should know about via Form 8-K within four business days. ***Data security increasingly represents an issue of vital importance to management, customers, and shareholders, with major corporate 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.
>
> I encourage you to investigate whether Yahoo and its senior executives fulfilled their obligations to keep investors and the public informed, and whether the company made complete and accurate representations about the security of its IT systems.[60]

[60]. https://www.warner.senate.gov/public/index.cfm/pressreleases?ContentRecord_id=AC6EC18E-F309-404B-BF2D-9F60CD9884E8

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

> ***We are even more disturbed that user information was first compromised in 2014, yet the company only announced the breach last week. That means millions of American's data may have been compromised for two years. This is unacceptable***. This breach is the latest in a series of data breaches that have impacted the privacy of millions of American consumers in recent years, but it is by far the largest. Consumers put their trust in companies when they share personal and sensitive information with them, and they expect all possible steps be taken to protect that information.
>
> In light of these troubling revelations, please answer the following questions to help Congress and the public better understand what went wrong and how Yahoo intends to safeguard data and protect its users, both now and in the future. We also request that Yahoo provide a briefing to our staff on the company's investigation into the breach, its interaction with appropriate law enforcement and national security authorities, and how it intends to protect affected users.
>
> 1. When and how did Yahoo first learn that its users' information may have been compromised? Please provide a timeline detailing the nature of the breach, when and how it was discovered, when Yahoo notified law enforcement or other government authorities about the breach, and when Yahoo notified its customers.
>
> 2. Press reports indicate the breach first occurred in 2014, but was not discovered until August of this year. If this is accurate, how could such a large intrusion of Yahoo's systems have gone undetected?
>
> 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?
>
> 7. What is Yahoo doing to prevent another breach in the future? Has Yahoo changed its security protocols, and in what manner?

> 8. Did anyone in the U.S. government warn Yahoo of a possible hacking attempt by state sponsored hackers or other bad actors? When was this warning issued?[61]

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

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

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

228. To date, ***Yahoo has not provided a cogent explanation why the Company took years to disclose the data breaches*** or who made the decision not to go public sooner with this information. Questions about the hacks persist to this day. It is not just the public that Defendants continue to stonewall, but U.S. Senators as well. Yahoo's representatives were supposed to meet with members of the Senate Commerce Committee on January 31, 2017. The Company abruptly canceled that meeting on January 28, 2017. Senators John Thune and Jerry Moran wrote to defendant Mayer expressing their dismay at this "last minute" cancellation. The Senators, in their letter, stated that the Company's last minute cancellation "***has prompted concerns about [Yahoo's] willingness to deal with Congress with***

[61] 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 .

complete candor about [the data breaches]." The letter stated that "[d]espite several inquiries by Committee staff seeking information about the security of Yahoo! user accounts, ***company officials have thus far been unable to provide answers to many basic questions***."[62]

229. In May 2017, Germany's federal cyber agency lambasted Yahoo for failing to cooperate with the agency's investigation into the hacking probes. The agency decided to publicly report Yahoo's stonewalling after Yahoo repeatedly refused to respond to efforts to analyze the data breaches and to prevent similar steps.[63]

The Breaches Jeopardized Yahoo's Transaction with Verizon

230. According to a September 26, 2016 New York Post article published soon after Yahoo disclosed the 2014 Data Breach, "Verizon is livid they were not informed [of the breach] during due diligence and in-fighting . . . is impacting the Yahoo deal and this could be the escape clause." The New York Post also reported that "[m]edia and tech bankers are already whispering that Verizon wants to get out of the Yahoo deal — and if they do they may pursue Twitter, which is now in play." The Post further reported that a source said that Verizon "would expect a price renegotiation at a minimum[.]"[64] The scope of the hack and its potential fallout, including the possibility of costly class-action lawsuits, reportedly prompted Verizon's renewed scrutiny of the deal. In a statement, Verizon said it would evaluate the situation "as the investigation continues through the lens of overall Verizon interests, including consumers, customers, shareholders and related communities."

---

[62] Robert McMillan, *Senators Question Yahoo's Candor on Data Breach*, Wall St. J. (Feb. 13, 2017, 9:41 a.m.). https://www.wsj.com/articles/senators-question-yahoos-candor-on-data-breach-1486788867.

[63] *German cyber agency chides Yahoo for not helping in hacking probes*, Business Recorder, May 15, 2017.

[64] *See* http://www.nypost.com/2016/09/26/yahoo-hack-may-send-verizon-running-from-potential-merger .

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

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

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

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

> The new disclosure could jeopardize Verizon's $4.83 billion acquisition of Yahoo's core internet business, a deal announced in July and expected to close in early 2017. In October, Verizon signaled it could consider the 2014 breach a material event that could allow it to change the deal terms.
>
> The companies were discussing the impact of that first breach when the second was discovered. Verizon learned of the latest breach in the past few weeks, a person familiar with the matter said. The company still has all options on the table, including renegotiating the deal's price or walking away, the person said.

235. Analysts highlighted that "Verizon has a fiduciary duty to its shareholders to at least demand a discount on the acquisition price," or it risks an "ignominious write off not unlike that 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."

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

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

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

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

Yahoo Faces Significant Financial Exposure and Reputational Harm

240. In the wake of the data breaches, Yahoo has disabled automatic email forwarding, preventing users who want to leave because of the recent hacking revelations from being able to switch to a rival service. Yahoo has reported that it is "work[ing] to improve" its email forwarding service, but information technology experts note that "[t]his is all extremely suspicious timing," especially given that email forwarding has been a service available to Yahoo users for over a decade and only now, and only at Yahoo, is it "under development."[65]

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

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

242. These actions and investigations subject Yahoo to significant financial exposure and reputational damage.

Materially False and Misleading Statements Issued During the Class Period

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

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

A. False and Misleading Statements Made in 2013

244. On or around April 30, 2013, Yahoo made the following public representations as part of its Privacy Policy, which the Company made available on its official website:[66]

> 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 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.

245. The statements referenced in ¶ 244 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(ii), (vii) and (xi) above.

246. On May 7, 2013, Yahoo filed a Quarterly Report on Form 10-Q with the SEC (the "Q1 2013 10-Q"). The Q1 2013 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.

[66] Yahoo represented that its Privacy Policy "covers how Yahoo treats personal information that 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."

> 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 cyberattacks), 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 unauthorized access, disable or degrade service, or sabotage systems change frequently 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 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.

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

248. The statements referenced in ¶ 246 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(ii), (vii) and (xi) above.

249. On August 8, 2013, Yahoo filed another Quarterly Report on Form 10-Q with the SEC (the "Q2 2013 10-Q"). The Q2 2013 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 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 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 unauthorized access, disable or degrade service, or sabotage systems change frequently 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 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.

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

251. The statements referenced in ¶ 249 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(iii), (vii) and (xi) above.

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

253. The statement referenced in ¶ 252 above was materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(iii), (vii) and (xi) above.

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

> At Yahoo, we take the security of our users very seriously. In a constantly changing digital environment, we recognize the need to continuously evaluate how to best protect your information.
>
> Yahoo Mail users can already enable https [or Secure Sockets Layer (SSL)], a communications protocol that securely encrypts your information and messages as they 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 and security.

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

> Starting January 8, 2014, we will make encrypted https connections standard for all Yahoo Mail users. Our teams are working hard to make the necessary changes to default https connections on Yahoo Mail, and we look forward to providing this extra layer of security for all our users.
>
> Yahoo will continue to enhance our security technology, policies and practices to provide the best possible protections for our users. We invite you to check out our Yahoo Security Center to learn about other steps you can take to help protect yourself online.
>
> UPDATE:
>
> In addition to making https a default feature by January 2014 for all Yahoo Mail users, we plan to implement 2048-bit encryption keys, which will provide our users with a further layer of security.

256. The statements referenced in ¶¶ 254-55 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(iii), (vii) and (xi) above.

257. On November 12, 2013, Yahoo filed a Quarterly Report on Form 10-Q with the SEC (the "Q3 2013 10-Q"). The Q3 2013 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 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 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 unauthorized access, disable or degrade service, or sabotage systems change frequently 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 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.

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

259. The statements referenced in ¶ 257 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(iii), (vii) and (xi) above.

260. On November 18, 2013, Yahoo posted on its official website the following statements made by Defendant Mayer, concerning Yahoo's commitment to protecting the personal information of its customers:

> We've worked hard over the years to earn our users' trust and we fight hard to preserve it . . .
>
> There is nothing more important to us than protecting our users' privacy. To that end, we recently announced that we will make Yahoo Mail even more secure by introducing https (SSL - Secure Sockets Layer) encryption with a 2048-bit key across our network by January 8, 2014.
>
> Today we are announcing that we will extend that effort across all Yahoo products. More specifically this means we will:
>
> - Encrypt all information that moves between our data centers by the end of Q1 2014;
> - Offer users an option to encrypt all data flow to/from Yahoo by the end of Q1 2014;
> - Work closely with our international Mail partners to ensure that Yahoo co-branded Mail accounts are https-enabled.
>
> As we have said before, we will continue to evaluate how we can protect our users' privacy and their data. We appreciate, and certainly do not take for granted, the trust our users place in us.

261. The statements referenced in ¶ 260 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(iii), (vii) and (xi) above.

262. On the same date, Defendant Mayer reinforced in her Twitter and Tumblr accounts "Yahoo's commitment to securing and encrypting (…) users' data."

263. The statement referenced in ¶ 262 above was materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(iii), (vii) and (xi) above.

B. False and Misleading Statements Made in 2014

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

> Yahoo is fully committed to keeping our users safe and secure online. As we promised back in October, we are now automatically encrypting all connections between our users and Yahoo Mail. Anytime you use Yahoo Mail - whether it's on the web, mobile web, 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.
>
> Security is a key focus for us and we'll continue to enhance our security technology and policies so we can provide a safe and secure experience for our users.

265. The statements referenced in ¶ 264 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(iv), (vii)-(viii), and (xi) above.

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

267. The statements referenced in ¶ 266 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(iv), (vii)-(viii), and (xi) above.

268. On February 28, 2014, Yahoo filed an Annual Report on Form 10-K with the SEC (the "2013 10-K"). The 2013 10-K 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 revenue, damage to our reputation, and potential liability. 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.

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

270. The statements referenced in ¶ 268 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(iv), (vii)-(viii), and (xi) above.

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

272. The Silicon Valley Business Journal enjoys wide public circulation and covers the latest news for professionals and others, including technology news, both online and in print. It also hosts a number of panels, events and awards presentations that are informative in nature. In addition to its 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.

273. The statements referenced in ¶ 271 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(iv), (vii)-(viii), and (xi) above.

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

> When I joined Yahoo four weeks ago, we were in the middle of a massive project to protect our users and their data through the deployment of encryption technologies as we discussed in our November 2013 Tumblr.
>
> So today, we're updating you on our progress:
>
> Traffic moving between Yahoo data centers is fully encrypted as of March 31.
>
> In January, we made Yahoo Mail more secure by making browsing over HTTPS the default. In the last month, we enabled encryption of mail between our servers and other mail providers that support the SMTPTLS standard.
>
> The Yahoo Homepage and all search queries that run on the Yahoo Homepage and most Yahoo properties also have HTTPS encryption enabled by default.
>
> We implemented the latest in security best-practices, including supporting TLS 1.2, 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.

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

> Hundreds of Yahoos have been working around the clock over the last several months to provide a more secure experience for our users and we want to do even more moving forward. Our goal is to encrypt our entire platform for all users at all time, by default.
>
> One of our biggest areas of focus in the coming months is to work with and encourage 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 only make Yahoo secure, but improve the security of the overall web ecosystem.
>
> In addition to moving all of our properties to encryption by default, we will be implementing additional security measures such as HSTS, Perfect Forward Secrecy and 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-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.

276. The statements referenced in ¶¶ 274-75 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(iv), (vii)-(viii), and (xi) above.

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

> The world has changed. So while email is an essential tool for business and personal life, it is also the focus for some of those who endeavor to do us harm. The new normal across the web can include massive attempts at account hacking, email spoofing (forging sender identity) and phishing attacks (tricking a user to give up account credentials).
>
> The doors to your inbox need another lock.
>
> Because of the rise of spoofing and phishing attacks, the industry saw a need over two years ago to require emails to be sent more securely and formed an organization, including Yahoo, Google, Aol, Microsoft, LinkedIn, and Facebook, to work out a solution. The organization designed and built something called DMARC, or Domain-based Message Authentication, Reporting and Conformance. Today, 80% of US email user accounts and over 2B accounts globally can be protected by the DMARC standard.
>
> On Friday afternoon last week, Yahoo made a simple change to its DMARC policy from "report" to "reject". In other words, we requested that all other mail services reject emails claiming to come from a Yahoo user, but not signed by Yahoo.
>
> Yahoo is the first major email provider in the world to adopt this aggressive level of DMARC policy on behalf of our users.
>
> And overnight, the bad guys who have used email spoofing to forge emails and launch phishing attempts pretending to come from a Yahoo Mail account were nearly stopped in their tracks . . .
>
> With stricter DMARC policies, users are safer, and the bad guys will be in a tough spot. More importantly, verified senders will unlock a massive wave of innovation and advancement for all our inboxes.

278. The statements referenced in ¶ 277 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(iv), (vii)-(viii), and (xi) above.

279. At Yahoo's April 15, 2014 Earnings Call for the first quarter of 2014, Defendant Mayer praised Yahoo's retention of Alex Stamos as the Company's VP of Information Security to strengthen security: "Alex Stamos joined Yahoo! as VP of Information Security. Alex brings vast information 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."

280. The statements referenced in ¶ 279 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(iv), (vii)-(viii), and (xi) above.

281. On May 8, 2014, Yahoo filed a Quarterly Report on Form 10-Q with the SEC (the "Q1 2014 10-Q"). The Q1 2014 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 revenue, damage to our reputation, and potential liability. 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.

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

283. The statements referenced in ¶ 281 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(iv), (vii)-(viii), and (xi) above.

284. On May 15, 2014, Yahoo posted on its official website the following statements from Alex Stamos, about Yahoo's ongoing commitments to put its "users first":

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

> ***I outlined specific ways we protect our users, including: our focus on security in the advertising pipeline; our leadership in the fight on email spam; the bug bounty program we operate; and our efforts to fully encrypt 100 percent of our network traffic.***
>
> Achieving security online is not an end state; it's a constantly evolving ***challenge*** that ***we tackle head on***. At Yahoo, we know that our users rely on us to help protect their information for them. We also see security as a partnership - we want to educate our users to be mindful of their own security habits, and we provide intuitive, user-friendly tools and security resources to help them do so.

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

> One reason I joined Yahoo is that from the top down, the company is devoted to protecting users. Building and maintaining trust through secure products is a critical focus for us, and by default all of our products should be secure for all of our users across the globe.
>
> Achieving security online is not an end state; it's a constantly evolving challenge that we tackle head on. At Yahoo, we know that our users rely on us to protect their information. We also see security as a partnership; we want to educate our users to be mindful of their own security habits, and we provide intuitive, user-friendly tools and security resources to help them do so.
>
> Malware is an important issue that is a top priority for Yahoo. While distribution of malware through advertising is one part of the equation, it's important to address the entire malware ecosystem and fight it at each phase of its lifecycle. It is also important to address security more broadly across the Internet.
>
> I outline in my testimony below several specific ways Yahoo is fighting criminals and 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.

286. 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.
>
> Yahoo also strives to keep deceptive advertisements from ever reaching users. For example, our systems prohibit advertisements that look like operating system messages, because such ads often tout false offers or try to trick users into downloading and installing malicious or unnecessary software. Preventing deceptive advertising once required

> extensive human intervention, which meant slower response times and inconsistent enforcement. Although no system is perfect, we now use sophisticated machine learning and image recognition algorithms to catch deceptive advertisements.
>
> This lets us train our systems about the characteristics of deceptive creatives, advertisers and landing sites so we detect and respond to them immediately.
> We are also the driving force behind the SafeFrame standard. The SafeFrame mechanism allows ads to properly display on a web page without exposing a user's private information to the advertiser or network. Thanks to widespread adoption, SafeFrame enhances user privacy and security not only in the thriving marketplace of thousands of publishers on Yahoo, but around the Internet.

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

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

288. Mr. Stamos also touted Yahoo's protection of private information through encryption. Yahoo posted this information on its official website:

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

289. The statements referenced in ¶¶ 284-88 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(iv), (vii)-(viii), and (xi) above.

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

> Here's a look at how we've had our users' back when it comes to security and transparency: . . .
>
> Encryption: In November 2013, we committed to introducing HTTPS (SSL - Secure Sockets Layer) encryption with 2048-bit keys across our network. We've made significant progress toward this goal, including:
>
> encrypting all data moving between our data centers;
>
> making browsing via Yahoo Mail HTTPS by default;
>
> ensuring that the Yahoo Homepage and all search queries run on the Yahoo Homepage and most Yahoo properties have HTTPS by default;
>
> implementing the latest in security best-practices, including supporting TLS 1.2, Perfect Forward Secrecy, and a 2048-bit RSA key for many of our global properties such as Homepage, Mail and Digital Magazines;
>
> empowering users to initiate an encrypted session for Yahoo News, Yahoo Sports, Yahoo Finance, and Good Morning America on Yahoo (gma.yahoo.com) by typing "https" before the site URL in their web browser;
>
> 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.

291. The statements referenced in ¶ 290 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(iv), (vii)-(viii), and (xi) above.

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

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

293. The statements referenced in ¶ 292 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(iv), (vii)-(viii), and (xi) above.

294. On August 7, 2014, Yahoo filed a Quarterly Report on Form 10-Q with the SEC (the "Q2 2014 10-Q"). The Q2 2014 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 revenue, damage to our reputation, and potential liability. 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.

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

296. The statements referenced in ¶ 294 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(iv), (vii)-(viii), and (xi) above.

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

- Detailed descriptions and mitigation instructions
- Accurate prioritization
- Consistent follow-up and real-time reporting
- Executive visibility
- Convincing company that you are a madman

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

299. The statements referenced in ¶¶ 297-98 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(iv), (vii)-(viii), and (xi) above.

300. On September 11, 2014, Yahoo posted on its official website the following statements from Ronald Bell: "Users come first at Yahoo . . . We are also committed to protecting users' data."

301. The statements referenced in ¶ 300 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(iv), (vii)-(viii), and (xi) above.

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

> 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.

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

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

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

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

> Updated to include data collection practices-Data Storage and Anonymization link:
>
> In addition to the other purposes for which we collect information, other types of log data (ie not relating to search) (such as ad views, ad clicks, page views and page clicks) are retained for a longer period in order to power innovative product development, provide personalized and customized services, and better able our security systems to 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.

305. The statements referenced in ¶¶ 302-04 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(iv), (vii)-(viii), and (xi) above.

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

307. The statement referenced in ¶ 306 above was materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(iv), (vii)-(viii), and (xi) above.

308. On November 7, 2014, Yahoo filed a Quarterly Report on Form 10-Q with the SEC (the "Q3 2014 10-Q"). The Q3 2014 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 revenue, damage to our reputation, and potential liability. 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.

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

310. The statements referenced in ¶ 308 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(iv), (vii)-(viii), and (xi) above.

C. False and Misleading Statements Made in 2015

311. On February 9, 2015, Yahoo posted on its official website the following statements from Lovlesh Chhabra, the Company's Product Manager:

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

312. The statements referenced in ¶ 311 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(v), (vii)-(ix), and (xi) above.

313. On February 27, 2015, Yahoo filed an Annual Report on Form 10-K with the SEC (the "2014 10-K"). The 2014 10-K 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 revenue, damage to our reputation, and potential liability. Outside parties may attempt to fraudulently induce employees, users, or customers to disclose sensitive information to gain access to our data or our users' or customers' data. In addition, hardware, software or applications we procure from third parties may contain defects in design or manufacture or other problems that could unexpectedly compromise network and data security. 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.

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

315. The statements referenced in ¶ 313 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(v), (vii)-(ix), and (xi) above.

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

> Q: Given Snowden and also the counterterrorism problem at the moment, how much has that raised much more questioning about your storage of say emails, in other words, how would you say Yahoo now stands on what we might call the trust index…?
>
> Mayer: . . . [T]he first thing that happened when [] we heard about Snowden's allegations is we changed the way that we store data, we changed the way that we communicate data, we went to entirely secure connections on all of the, Yahoo's major properties hgtps, we changed the way we did encryption between the data centers to basically get a more secure environment for our end users because we realized that's what they wanted. So we changed all of those things in response to those allegations.
>
> Q: And what was the impact on trust?
>
> Mayer: We didn't have a measurement necessarily before, but the measurement afterwards shows that people's trust and their confidence in the service has rebounded as a result of it they understand that now that we're using more secure protocols to communicate and to transfer their data.
>
> * * *
>
> I would just make the observation that protection and trust really come as a function of security and privacy, but there is a tension between those two.
>
> * * *
>
> Mayer: …whether or not they're coming through the official system to get data, they are in fact getting data and so we can do what we can do in order to protect our users, which is usually through encryption methods and the like . . . .

317. The statements referenced in ¶ 316 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(v), (vii)-(ix), and (xi) above.

318. 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.
>
> Just a few years ago, e2e encryption was not widely discussed, nor widely understood. Today, our users are much more conscious of the need to stay secure online. There is a wide spectrum of use for e2e encryption, ranging from the straightforward (sharing tax forms with an accountant), to the potentially life-threatening (emailing in a country that does not respect freedom of expression). Wherever you land on the spectrum, we've heard you loud and clear: We're building the best products to ensure a more secure user experience and overall digital ecosystem.

319. The statements referenced in ¶ 318 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(v), (vii)-(ix), and (xi) above.

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

> Our Users First Approach in Action
> Protecting Users . . .
>
> We've encrypted many of our most important products and services to protect against snooping by governments or other actors. This includes:
>
> Encryption of the traffic moving between Yahoo data centers;
>
> Making browsing over HTTPS the default on Yahoo Mail and Yahoo Homepage;
>
> Implementing the latest in security best-practices, including supporting TLS 1.2, Perfect Forward Secrecy and a 2048-bit RSA key for many of our global properties such as Homepage, Mail, and Digital Magazines; and
>
> We've also rolled out an end-to-end (e2e) encryption extension for Yahoo Mail, now available on GitHub. We are committed to the security of this solution and oppose mandates to deliberately weaken it or any other cryptographic system.
>
> We are committed to notifying users when we strongly suspect they may have been the target of a state-sponsored attack.

321. The statements referenced in ¶ 320 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(v), (vii)-(ix), and (xi) above.

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

323. The statements referenced in ¶ 322 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(v), (vii)-(ix), and (xi) above.

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

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

325. The statements referenced in ¶ 324 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(v), (vii)-(ix), and (xi) above.

326. On May 7, 2015, Yahoo filed a Quarterly Report on Form 10-Q with the SEC (the "Q1 2015 10-Q"). The Q1 2015 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 revenue, damage to our reputation, and potential liability. Outside parties may attempt to fraudulently induce employees, users, or customers to disclose sensitive information to gain access to our data or our users' or customers' data. In addition, hardware, software or applications we procure from third parties may contain defects in design or manufacture or other problems that could unexpectedly compromise network and data security. 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.

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

328. The statements referenced in ¶ 326 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(v), (vii)-(ix), and (xi) above.

329. On July 22, 2015, in a conference call with investors, Defendant Mayer stated that at Yahoo, "we continue to protect our mail users with new investments in spam and phishing detection."

330. The statements referenced in ¶ 329 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(v), (vii)-(ix), and (xi) above.

331. On August 7, 2015, Yahoo filed a Quarterly Report on Form 10-Q with the SEC (the "Q2 2015 10-Q"). The Q2 2015 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 revenue, damage to our reputation, and potential liability. Outside parties may attempt to fraudulently induce employees, users, or customers to disclose sensitive information to gain access to our data or our users' or customers' data. In addition, hardware, software or applications we procure from third parties may contain defects in design or manufacture or other problems that could unexpectedly compromise network and data security. 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.

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

333. The statements referenced in ¶ 331 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(v), (vii)-(ix), and (xi) above.

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

> At Yahoo, we're committed to protecting our users' security, and we're proud that our network supports HTTPS across the board . . .
>
> Since we first began deploying encryption technologies across our network, we've worked with 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. This 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.

335. The statements referenced in ¶ 334 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(v), (vii)-(ix), and (xi) above.

336. At Yahoo's October 20, 2015 Earnings Call for the third quarter of 2015, Defendant Mayer lauded Yahoo's new e-mail security features:

> Just last week, we launched the new Yahoo! Mail mobile application to an extremely positive reception. In addition to focusing on back end improvements to improve speed and performance, we also refreshed the design, making Mail more beautiful and intuitive. We introduced multiple account support, making it easier for users to access their other e-mail accounts directly from Yahoo! Mail, and we took an industry-leading step towards a password-free future with the announcement of Yahoo! Account Key, which pushes notifications to your phone to provide a fast, convenient, and secure way to access your Yahoo! accounts without having to memorize a password. This also makes it significantly easier to protect our users' accounts going forward.

337. The statements referenced in ¶ 336 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(v), (vii)-(ix), and (xi) above.

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

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

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

341. The statements referenced in ¶¶ 338-39 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(v), (vii)-(ix), and (xi) above.

342. On November 5, 2015, Yahoo filed a Quarterly Report on Form 10-Q with the SEC (the "Q3 2015 10-Q"). The Q3 2015 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 revenue, damage to our reputation, and potential liability. Outside parties may attempt to fraudulently induce employees, users, or customers to disclose sensitive information to gain access to our data or our users' or customers' data. In addition, hardware, software

> or applications we procure from third parties may contain defects in design or manufacture or other problems that could unexpectedly compromise network and data security. 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.

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

344. The statements referenced in ¶ 342 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(v), (vii)-(ix), and (xi) above.

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

> 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 product 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.

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

> Yahoo does not rent, sell, or share personal information about you with other people or non-affiliated companies except to provide products or services you've requested, when we have your permission, or under the following circumstances:
>
> > We provide the information to trusted partners who work on behalf of or with Yahoo under confidentiality agreements. These companies may use your personal information to help Yahoo communicate with you about offers from Yahoo and our marketing partners. However, these companies do not have any independent right to share this information.

> We have a parent's permission to share the information if the user is a child under age 13. See Children's Privacy & Family Accounts for more information about our privacy practices for children under 13.
>
> We respond to subpoenas, court orders, or legal process (such as law enforcement requests), or to establish or exercise our legal rights or defend against legal claims.
>
> We believe it is necessary to share information in order to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of Yahoo's terms of use, or as otherwise required by law.
>
> We transfer information about you if Yahoo is acquired by or merged with another company. In this event, Yahoo will notify you before information about you is transferred and becomes subject to a different privacy policy.

347. 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)
> > We use TLS encryption when transmitting certain kinds of information, such as financial services information or payment information. An icon resembling a padlock is displayed in most browsers during TLS sessions.
> >
> > Second Sign-in Verification
> > You may turn on a setting that requires a second piece of information such as a code sent via SMS - in addition to your password - when signing in to your account from a device or location we don't recognize. (…).
> >
> > On-Demand Passwords
> > Yahoo also offers on-demand passwords. By linking your mobile device to your account, you enable Yahoo to provide you with an on-demand password sent to your mobile phone, so you don't have to remember passwords anymore. (…).
> >
> > Secure Storage
> > We deploy industry standard physical, technical, and procedural safeguards that comply with relevant regulations to protect your personal information.
> >
> > Vendors and Partners
> > To protect the security and privacy of your information, we may provide information to partners and vendors who work on our behalf or with us under confidentiality agreements. These companies do not have any independent right to use or share this information without your consent.
> >
> > Access to Information

> We limit access to personal information about you to those employees who we reasonably believe need to come into contact with that information to provide products or services to you or in order to process this information for us.
>
> Education and Training
> We have implemented a company-wide education and training program about security that is required of every Yahoo employee.

348. The statements referenced in ¶¶ 345-47 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(v), (vii)-(ix), and (xi) above.

D. False and Misleading Statements Made in 2016

349. On February 29, 2016, Yahoo filed an Annual Report on Form 10-K with the SEC (the "2015 10-K"). The 2015 10-K 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 revenue, damage to our reputation, and potential liability. Outside parties may attempt to fraudulently induce employees, users, or customers to disclose sensitive information to gain access to our data or our users' or customers' data. In addition, hardware, software or applications we procure from third parties may contain defects in design or manufacture or other problems that could unexpectedly compromise network and data security. Additionally, some third parties, such as our distribution partners, service providers and vendors, and app developers, may receive or store information provided by us or by our users through applications integrated with Yahoo. If these third parties fail to adopt or adhere to adequate data security practices, or in the event of a breach of their networks, our data or our users' data may be improperly accessed, used or disclosed. Security breaches or unauthorized access have resulted in and may in the future result in a combination of significant legal and financial exposure, increased remediation and other costs, damage to our reputation and a loss of confidence in the security of our products, services and networks that could have an adverse effect on our business. We take steps to prevent unauthorized access to our corporate systems, however, because the techniques used to obtain unauthorized access, disable or degrade service, or sabotage systems change frequently or may be designed to remain dormant until a triggering event, we may be unable to anticipate these techniques or implement adequate preventative measures. If an actual or perceived breach of our security occurs, the market perception of the effectiveness of our security measures could be harmed and we could lose users and customers.

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

351. The statements referenced in ¶ 349 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(xi) above.

352. On March 3, 2016, Yahoo published on its official website statements made by Ron Bell, observing that "[m]ore than 1 billion users entrust their personal information to Yahoo. [The 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***."

353. The statements referenced in ¶ 352 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(xi) above.

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

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

355. The statements referenced in ¶ 354 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(xi) above.

356. On May 10, 2016, Yahoo filed a Quarterly Report on Form 10-Q with the SEC (the "Q1 2016 10-Q"). The Q1 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 revenue, damage to our reputation, and potential liability. Outside parties may attempt to fraudulently induce employees, users, or customers to disclose sensitive information to gain access to our data or our users' or customers' data. In addition, hardware, software or applications we procure from third parties may contain defects in design or manufacture or other problems that could unexpectedly compromise network and data security. Additionally, some third parties, such as our distribution partners, service providers and vendors, and app developers, may receive or store information provided by us or by our users through applications integrated with Yahoo. If these third parties fail to adopt or adhere to adequate data security practices, or in the event of a breach of their networks, our data or our users' data may be improperly accessed, used or disclosed. Security breaches or unauthorized access have resulted in and may in the future result in a combination of significant legal and financial exposure, increased remediation and other costs, damage to our reputation and a loss of confidence in the security of our products, services and networks that could have an adverse effect on our business. We take steps to prevent unauthorized access to our corporate systems, however, because the techniques used to obtain unauthorized access, disable or degrade service, or sabotage systems change frequently or may be designed to remain dormant until a triggering event, we may be unable to anticipate these techniques or implement adequate preventative measures. If an actual or perceived breach of our security occurs, the market perception of the effectiveness of our security measures could be harmed and we could lose users and customers.

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

358. The statements referenced in ¶ 356 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(xi) above.

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

> [A]ny 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. 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.

360. The statements referenced in ¶ 359 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(xi) above.

361. On August 8, 2016, Yahoo filed a Quarterly Report on Form 10-Q with the SEC (the "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 revenue, damage to our reputation, and potential liability. Outside parties may attempt to fraudulently induce employees, users, or customers to disclose sensitive information to gain access to our data or our users' or customers' data. In addition, hardware, software or applications we procure from third parties may contain defects in design or manufacture or other problems that could unexpectedly compromise network and data security. Additionally, some third parties, such as our distribution partners, service providers and vendors, and app developers, may receive or store information provided by us or by our users through applications integrated with Yahoo. If these third parties fail to adopt or adhere to adequate data security practices, or in the event of a breach of their networks, our data or our users' data may be improperly accessed, used or disclosed. Security breaches or unauthorized access have resulted in and may in the future result in a combination of significant legal and financial exposure, increased remediation and other costs, damage to our reputation and a loss of confidence in the security of our products, services and networks that could have an adverse effect on our business. We take steps to prevent unauthorized access to our corporate systems, however, because the techniques used to obtain unauthorized access, disable or degrade service, or sabotage systems change frequently or may be designed to remain dormant until a triggering event, we may be unable to anticipate these techniques or implement adequate preventative measures. If an actual or perceived breach of our security occurs, the market perception of the

> effectiveness of our security measures could be harmed and we could lose users and customers.

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

363. The statements referenced in ¶ 361 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(xi) above.

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

> 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.

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

> Yahoo does not rent, sell, or share personal information about you with other people or non-affiliated companies except to provide products or services you've requested, when we have your permission, or under the following circumstances:
>
> > We provide the information to trusted partners who work on behalf of or with Yahoo under confidentiality agreements. These companies may use your personal information to help Yahoo communicate with you about offers from Yahoo and our marketing partners. However, these companies do not have any independent right to share this information.
> >
> > We have a parent's permission to share the information if the user is a child under age 13. See Children's Privacy & Family Accounts for more information about our privacy practices for children under 13.
> >
> > We respond to subpoenas, court orders, or legal process (such as law enforcement requests), or to establish or exercise our legal rights or defend against legal claims.
> >
> > We believe it is necessary to share information in order to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of Yahoo's terms of use, or as otherwise required by law.

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

366. Yahoo's August 2016 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)
> We use TLS encryption when transmitting certain kinds of information, such as financial services information or payment information. An icon resembling a padlock is displayed in most browsers during TLS sessions.
>
> Second Sign-in Verification
> You may turn on a setting that requires a second piece of information such as a code sent via SMS - in addition to your password - when signing in to your account from a device or location we don't recognize. (…)
>
> On-Demand Passwords
> Yahoo also offers on-demand passwords. By linking your mobile device to your account, you enable Yahoo to provide you with an on-demand password sent to your mobile phone, so you don't have to remember passwords anymore. (…)
>
> Secure Storage
> We deploy industry standard physical, technical, and procedural safeguards that comply with relevant regulations to protect your personal information.
>
> Vendors and Partners
> To protect the security and privacy of your information, we may provide information to partners and vendors who work on our behalf or with us under confidentiality agreements. These companies do not have any independent right to use or share this information without your consent.
>
> Access to Information
> We limit access to personal information about you to those employees who we reasonably believe need to come into contact with that information to provide products or services to you or in order to process this information for us.
>
> Education and Training
> We have implemented a company-wide education and training program about security that is required of every Yahoo employee. (…)
>
> Please note that no data transmission over the Internet or information storage technology can be guaranteed to be 100% secure. We continue to evaluate and implement enhancements in security technology and practices.

367. The statements referenced in ¶¶ 364-66 above were materially false and/or misleading for the reasons set forth in ¶ 243 (i)-(xi) above.

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

> [T]here 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. 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.

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

370. The statements referenced in ¶ 368 above were materially false and/or misleading for the reasons set forth in ¶ 243 (vii)-(x) above.

371. On September 22, 2016, Yahoo issued a press release providing information to users regarding the 2014 Data Breach, which was filed as an exhibit to the Company's Form 8-K (the "September 22, 2016 Press Release"). The September 22, 2016 Press Release stated, in part:

> *A recent investigation by Yahoo! Inc.* (NASDAQ: YHOO) has confirmed that a copy of certain user account information was stolen from the [C]ompany's network in late 2014 by what it believes is a state-sponsored actor. The account information *may have* included

> names, email addresses, telephone numbers, dates of birth, hashed passwords (the vast majority with bcrypt) and, in some cases, encrypted and unencrypted security questions and answers.

372. The statements referenced in ¶ 371 above were materially false and/or misleading for the reasons set forth in ¶¶ 186, 188-89 above.

The Truth Begins to Emerge

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

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

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

> Below are some key data points from our Bug Bounty program to date, which we'll continue to update to help the security community understand the efficacy of this work and help focus research in this space:
>
> - To date, we've paid out +$1M to security vulnerability reporters.
> - Submissions since the inception of the program have now reached the 10,000 mark.
> - Approximately 1,500 of these 10,000 reports have resulted in a bounty payout.
> - The current monthly validity rate of submissions is around 15%, an increase from 10% at the end of 2014.
> - More than 1,800 reporters have participated in the program, about 600 of these have reported verifiable bugs.
> - 50% of the submissions are from the top 6% set of contributors.
> - 87% of researchers submit less than 10 bugs, this equates to about 34% of all submissions.

376. 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.

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

> The news of Martinez departing Yahoo and joining Apple had not been announced but the details are confirmed in his LinkedIn profile, which notes that he joined Apple in August of this year as part of the Cupertino company's information security team.
>
> Reached for comment, Yahoo says that it is currently looking for a permanent CISO. "SVP Jay Rossiter is guiding our security team while we continue our search for Yahoo's next CISO," said a spokesperson for the company.
>
> Martinez had only been appointed to the role in July, when the former CISO, Alex Stamos, was poached by Facebook. He had been with the company since 2011.
>
> At a time when cybersecurity has been a[n] increasing issue due to hacking incidents and developments involving the NSA and snooping by government authorities, Martinez oversaw a number of security initiatives at Yahoo.
>
> They included the company corporate incident response policy, risk analysis process, threat matrix, and standards; creating and managing the company's global incident response program; liaising with law enforcement during security incidents and investigations; and founding and managing the company's bug bounty program.

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

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

380. On December 2, 2015, the New York Times reported that the Board of Yahoo would hold a series of meetings to review the possibility of selling its main business. The New York Times report came after Yahoo shareholder Starboard Value LP urged the Company to drop its plans to hive 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 reported that Yahoo shares had fallen in price after reports that Alibaba was not interested in Yahoo's core business.

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

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

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

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

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

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

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

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

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

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

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

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

393. On this news, Yahoo's share price fell $1.06, or 2.69%, to close at $38.32 on July 25, 2016.

394. On the morning of September 22, 2016, investors learned that a massive data breach had occurred at Yahoo. *Recode* reported that the Company was about to confirm a large-scale theft of Yahoo user data.[67]

> Yahoo is poised to confirm a massive data breach of its service, according to several sources close to the situation. The company was the victim of hacking that has exposed several hundred million user accounts.
>
> While sources were unspecific about the extent of the incursion, since there is the likelihood of government investigations and legal action related to the breach, they noted that it is widespread and serious.
>
> Earlier this summer, Yahoo said it was investigating a data breach in which hackers claimed to have access to 200 million user accounts and one was selling them online. "It's as bad as that," said one source. "Worse, really."

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

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

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

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

In the afternoon of the same day, Yahoo issued a press release confirming it had been hacked.[68] Yahoo

[67] 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.

[68] *An Important Message to Yahoo Users on Security*, *Business Wire*, Sept. 22, 2016, 2:28 pm ET.

admitted that "information associated with at least 500 million user accounts was stolen" from its network "in late 2014 by what it believes is a state-sponsored actor." This information "may have included names, email addresses, telephone numbers, dates of birth, hashed passwords…and, in some cases, encrypted or unencrypted security questions and answers." Yahoo also recommended that "users who haven't changed their passwords since 2014 do so."

395. Yahoo's revelations about the breach, described in news reports as "the largest ever disclosed," prompted questions from senior government figures and the media about the timing of Yahoo's response. On September 22, 2016, *Dow Jones* reported: [69]

> The Yahoo breach, and the timing of the disclosure, quickly reverberated in Washington. Sen. Mark Warner, D-Va., said in a statement, "I am perhaps most troubled by news that this breach occurred in 2014, and yet the public is only learning details of it today."[70]

Following Yahoo's confirmation of the breach, *Recode* questioned the timeliness of Yahoo's disclosures.

> Why did it take two years to discover and/or disclose the breach? What other breaches have there been? Who made the decision not to warn users and urge systemwide password resets? And, of course, why didn't management make the dire situation more clear to bidders for Yahoo's core business, which is the part of the company impacted?[71]

396. Analysts repeatedly observed during the Class Period that Yahoo's stock price was greatly affected by Alibaba Group Holding Limited ("Alibaba"),[72] the Chinese e-commerce giant which traded in the U.S., in which Yahoo held a significant stake which was Yahoo's largest asset.[73] On September

---

[69] *Yahoo Says Breach Affected at Least 500 Million Users*, Dow Jones Newswires, Sept. 22, 2016, 2:50 pm ET.

[70] *Id.*

[71] 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.

[72] *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.

[73] *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* Yahoo! Inc. Form 10-K for the year ended December 31, 2015, filed Feb. 29, 2016, p. 39.

22, 2016, news also reached the market that two analysts (Stifel and UBS) had increased their price targets and made positive comments on Alibaba.[74] On September 22, 2016, Alibaba's share price closed at $109.36, up from a closing price of $106 on September 21, 2016, an increase of $3.36 or 3.17%.

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

398. News coverage and analysis of Yahoo's data breach continued after market close on September 22 and through September 23, 2016. *Agence France Presse* reported Yahoo "was under pressure Friday to explain how it sustained such a massive breach in 2014, which possibly affected 500 million accounts."[75] Criticism of Yahoo grew, including from international authorities and from data security experts. *Computer Weekly* reported action by the U.K.'s Information Commissioner.[76]

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

---

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

[75] G. Jackson, L. Benhamou, *Russia? China? Who hacked Yahoo, and why?*, *Agence France Presse*, Sept. 23, 2016, 9:27 am ET.

[76] W. Ashford, Security Editor, *Yahoo under fire over data breach affecting 500 million users*, Computer Weekly, Sept. 23, 2016, 10:45 am ET.

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

Experts in data security questioned when Yahoo was aware of the data theft and how the theft could have gone unreported for so long, as reported by media, including *Computer Weekly*.[77]

> While Yahoo has confirmed the breach took place in late 2014, it has not made it clear exactly when it became aware of the breach, said Keatron Evans, senior security researcher at Blink Digital Security.
>
> "If it happened in 2014, and the company has known about it for the past two years, then why has it taken so long to reveal the extent of the breach?"
>
> ….Troy Gill, manager of security research at AppRiver, said …"I would be interested to know the findings by Yahoo when they allegedly investigated the 200 million records that were for sale on the dark web. Were the records confirmed as valid? If so, why did it take this long to inform users of the breach and why were no forced password resets issued prior?"
>
> ….Michael Lipinski, CISO and chief security strategist at Securonix, said …"We can't keep accepting this level of ignorance as the best we can do"…adding that he does not believe it took two years to find the breach.
>
> "With the Verizon acquisition in process, there is this thing called due diligence that happens. I firmly believe that this is only now coming to light due to that due diligence. I believe someone knew about this earlier," said Lipinski.
>
> "Whether there was a cover up or if this breach was not uncovered for two years, this is a huge failure of the Yahoo team for not being able to identify this much earlier," he said.
>
> Lipinski said the Yahoo security team appears to be trying to deflect the risk to users by saying that passwords were hashed using bcrypt.
>
> "Ask them how that worked out for Ashley Madison. They used the same salt hash and the hackers found a work around to the brute force methods of cracking the password," he said.

399. 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%.

400. 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.

[77] *Id.*

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

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

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

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

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

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

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

408. After market close on December 14, 2016, Yahoo revealed a data breach far larger than any it had disclosed before, affecting "more than one billion user accounts."[78]

> 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 associated with this theft. Yahoo believes this incident is likely distinct from the incident the company disclosed on September 22, 2016.
>
> ….Yahoo is notifying potentially affected users and has taken steps to secure their accounts, including requiring users to change their passwords.

On the next trading day, December 15, 2016, Yahoo's share price reacted quickly to these disclosures. In the morning, *Bloomberg* reported the resulting decline in price of Yahoo shares, as well as analysts' comments on the effect the latest news of a security breach would have on the deal to sell Yahoo's core business to Verizon.[79]

> Yahoo! Inc. fell Thursday after disclosing a second major security breach that may have affected more than 1 billion user accounts, a development that some analysts say may lead Verizon Communications Inc. to reconsider its bid for the main web businesses.
>
> The revelation may drive the market to consider a higher probability of Verizon walking away or renegotiating the $4.8 billion deal price, wrote Joseph Stauff, an analyst at Susquehanna Financial Group, in a note to clients. The shares fell as much as 3.8 percent, to $39.37, the biggest drop in a month.

Bloomberg reported Verizon was in fact said to be exploring changes to its deal with Yahoo following confirmation of this second major breach.[80]

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

---

[78] *Important Security Information for Yahoo Users*, Business Wire, Dec. 14, 2016, 4:51 pm EST.

[79] S. Moritz and B. Womack, *Yahoo Falls After Hack Raises Possibility Verizon May Reconsider*, *Bloomberg News*, Dec. 15, 2016, 10:28 am ET.

[80] 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.

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

According to *The Financial Times*, in reaction to the biggest data breach ever reported, "Yahoo shares dropped 5 percent on Thursday amid worries that the latest hacking revelations could scuttle its deal with Verizon Communications."[81]

> California-based Yahoo revealed on Wednesday that information on more than 1bn users was stolen in 2013, representing by far the biggest ever data breach. It follows revelations earlier this year in September about an apparently separate hack that took place in 2014 and affected 500m users.
>
> The news has once again put Verizon's deal to buy the company in the spotlight, with Bloomberg News reporting that the US telecommunications company is weighing whether to scrap the deal completely.
>
> Yahoo's shares were off by as much as 6.5 per cent following the Bloomberg headlines.
>
> "(W)e think that Verizon has a fiduciary duty to its shareholders to at least demand a discount on the acquisition price," said Richard Windsor, analyst at Edison Investment Research.

U.S. and international government figures were critical of Yahoo and demanded explanations for this second and even larger data breach, according to *The Financial Times*.[82]

> Ms. Mayer is also facing serious questions from regulators on both sides of the Atlantic concerned about the sophistication of the company's cyber defences and how long it took to detect the intruder.
>
> Mark Warner, a US senator, said it was "deeply troubling" that consumers were first 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.
>
> Regulators in the UK and in Ireland, where Yahoo has its European headquarters, have demanded further details from the company about how their citizens have been affected…..
>
> "We are urgently examining the facts that have been made available to us," said Helen Dixon, data protection commissioner of Ireland, "in order to ascertain the further investigative questions we need to pose and steps to be taken in order to ultimately conclude if European data protection laws have been breached."

[81] 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.

[82] 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.

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

410. On December 18, 2016, Reuters reported that Yahoo used encryption protocol MD5, which was considered inadequate by security professionals, for years before the Company finally changed to better encryption in the wake of the 2013 breach. In 2008, Carnegie Mellon warned security professionals through U.S. government alert systems that MD5 was unsuitable for further use. On this news, Yahoo's share price fell $0.19, or 0.49%, to close at $38.42 on December 19, 2016.

411. On January 5, 2017, Reuters reported that a senior Verizon executive said that the Company was unsure about its planned acquisition of Yahoo. While the merits of the deal still made sense, there were certain aspects of the investigation that had yet to be completed. The executive did not provide a time-frame for the completion of the deal.

412. On this news, Yahoo's share price fell $0.11, or 0.27%, to close at $41.23 on January 6, 2017.

ADDITIONAL SCIENTER ALLEGATIONS

413. In addition to the foregoing, certain of the Individual Defendants' actual knowledge of the falsity of the alleged misstatements is established by their signing of certifications pursuant to Section 302 of the Sarbanes-Oxley Act of 2002, which certified that the SEC filings "do[] not contain any untrue statement of a material fact or omit to state a material fact necessary to make the statements made, in light of the circumstances under which such statements were made, not misleading." Before vouching for the accuracy of the statements made in Yahoo's SEC filings, the certifying Defendants were obligated to familiarize themselves with the contents of the filings and the underlying operations of Yahoo described therein.

414. The Individual Defendants who made, signed, or otherwise were quoted in the other statements to investors described herein, who thereby presented themselves as knowledgeable about the

subject matter thereof, were under a similar obligation to familiarize themselves with the subject matter of those statements to ensure that they conveyed complete, truthful, and non-misleading information.

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

(a) By choosing to speak on the topics and subjects outlined herein, in the allegedly false and misleading statements described herein, Defendants had a duty to familiarize themselves with the subject matter thereof and a correlating duty to speak accurately and completely about it;

(b) By choosing to disclose information about these topics and subjects, Defendants were under a duty to disclose the whole truth;

(c) In any instance where Defendants made partial disclosures that conveyed false impressions, they had a duty to disclose the whole truth;

(d) To the extent that new information later arose that made any of Defendants' earlier alleged misstatements misleading or untrue, Defendants were obligated to disclose the whole truth and to correct their prior misstatements.

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

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

- Defendants admitted that they had contemporaneous knowledge of the breaches. For example, on March 1, 2017, Yahoo admitted that "the Company's information security team had contemporaneous knowledge of the 2014 compromise of user accounts, as well as incidents by

the same attacker involving cookie forging in 2015 and 2016. In late 2014, senior executives and relevant legal staff were aware that a state-sponsored actor had accessed certain user accounts by exploiting the Company's account management tool." Concurrently with this admission, Yahoo penalized Defendants Bell and Mayer in connection with the hacking incidents. For example, Yahoo announced "management changes," including the Board's decision not to award Defendant Mayer a cash bonus for 2016; Mayer's "offer" to forego any 2017 annual equity awards; and Bell's resignation as General Counsel and from all other positions with the Company without pay.

- The FBI agents intricately involved in the investigation of the 2014 Data Breach specifically singled out Defendant Mayer for her ongoing two-year involvement (since 2014) in the investigation.
- The FBI, who worked closely with Defendants from the beginning of the 2014 Data Breach, immediately noticed evidence that the hackers were affiliated with a Russian intelligence agency. The British intelligence agency was summoned to help the U.S. probe because the actions of Russia's hackers were classified as "hostile."
- Yahoo admitted that "as of December 2014, the information security team, which included Defendant Stamos, understood that the attacker had exfiltrated copies of user database backup files containing the personal data of Yahoo users . . . "
- Yahoo's Board of Directors, including Defendant Mayer, regularly received updates from the Company's Chief Information Security Officers, including Defendant Stamos, about cybersecurity updates, during many meetings, including meetings held on April 8, 2014, June 25, 2014, October 16, 2014, June 23, 2015, October 14-15, 2015, and April 13-14, 2016. The Board, including Defendant Mayer, had knowledge of and received regular updates on the 2014 Data Breach starting at least as early as October 2014 and continuing until at least April 2016.

- Confidential witnesses corroborate that Defendants knew of the 2013 and 2014 breaches soon after they occurred and years before they were publicly disclosed. CW1 stated that Defendant Mayer received daily updates of the breaches. Yahoo was trying to trouble shoot the hacked email accounts during both the 2013 and 2014 breaches. According to CW1, Mayer did not want to publicize the breaches.
- Despite knowing that Yahoo had been a target of nation-state spies, including repeated attacks by Russian hackers, Defendant Mayer refused to implement even the most rudimentary security measures, frequently clashing with Defendant Stamos "for fear that even something as simple as a password change would drive Yahoo's shrinking email users to other services."
- Defendants rejected requests for assistance from third party intelligence officers who independently identified a group of hackers claiming to have possession of a database of logins for up to three billion Yahoo accounts, for fear of jeopardizing the Verizon transaction. Yahoo employed a similar dismissive approach in connection with the 2014 Data Breach, refusing to confirm a notorious hacker's claim in July 2016 that he was in possession of account names and passwords of 200 million Yahoo users. Only after the Verizon deal was sealed did Yahoo belatedly acknowledge that a state-sponsored hack affected more than 500 million Yahoo accounts.
- Despite their concurrent knowledge of the 2013, the 2014, and the Forged Cookies data breaches, Defendants falsely represented in a September 9, 2016 regulatory filing with the SEC that "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 Yahoo's possession.

PLAINTIFFS' CLASS ACTION ALLEGATIONS

418. Plaintiffs bring this action as a class action pursuant to Federal Rule of Civil Procedure 23(a) and (b)(3) on behalf of a Class, consisting of all those who purchased or otherwise acquired Yahoo common shares traded on the NASDAQ during the Class Period (the "Class") and were damaged upon the revelation of the alleged corrective disclosures. Excluded from the Class are Defendants herein, the officers and directors of the Company, at all relevant times, members of their immediate families and their legal representatives, heirs, successors or assigns and any entity in which Defendants have or had a controlling interest.

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

420. Plaintiffs' claims are typical of the claims of the members of the Class as all members of the Class are similarly affected by Defendants' wrongful conduct in violation of federal law that is complained of herein.

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

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

- whether the federal securities laws were violated by Defendants' acts as alleged herein;
- 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.

423. 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.

424. 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.

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

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

COUNT I

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

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

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

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

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

- employed devices, schemes and artifices to defraud;
- made untrue statements of material facts or omitted to state material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; or

- engaged in acts, practices and a course of business that operated as a fraud or deceit upon Plaintiffs and others similarly situated in connection with their purchases of Yahoo common shares during the Class Period.

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

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

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

434. Had Plaintiffs and the other members of the Class been aware that the market price of Yahoo securities had been artificially and falsely inflated by Yahoo and the Individual Defendants' misleading statements and by the material adverse information which Yahoo and the Individual Defendants did not disclose, they would not have purchased Yahoo's common shares at the artificially inflated prices that they did, or at all.

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

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

COUNT II

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

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

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

439. As officers and/or directors of a publicly owned company, the Individual Defendants had a duty to disseminate accurate and truthful information with respect to Yahoo's data safety and

operations, and to correct promptly any public statements issued by Yahoo which had become materially false or misleading.

440. Because of their positions of control and authority as senior officers, the Individual Defendants were able to, and did, control the contents of the various reports, statements, press releases and public filings which Yahoo disseminated in the marketplace during the Class Period. Throughout the Class Period, the Individual Defendants exercised their power and authority to cause Yahoo to engage in the wrongful acts complained of herein. The Individual Defendants, therefore, were "controlling persons" of Yahoo within the meaning of Section 20(a) of the Exchange Act. In this capacity, they participated in the unlawful conduct alleged, which artificially inflated the market price of Yahoo common shares.

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs demand judgment against Defendants as follows:

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

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

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

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

DEMAND FOR TRIAL BY JURY

Plaintiffs hereby demand a trial by jury.

Dated: February 2, 2018

Respectfully submitted,

POMERANTZ LLP

By: */s/ Jeremy A. Lieberman*
Jeremy A. Lieberman
Emma Gilmore
Michael Grunfeld
600 Third Avenue, 20th Floor
New York, New York 10016
Telephone: (212) 661-1100
Facsimile: (212) 661-8665
Email: jalieberman@pomlaw.com
Email: egilmore@pomlaw.com

POMERANTZ LLP
Patrick V. Dahlstrom
Ten South La Salle Street, Suite 3505
Chicago, Illinois 60603
Telephone: (312) 377-1181
Facsimile: (312) 377-1184
Email: pdahlstrom@pomlaw.com

GLANCY PRONGAY & MURRAY LLP
Joshua L. Crowell
Jennifer Leinbach
1925 Century Park East, Suite 2100
Los Angeles, California 90067
Telephone: (310) 201-9150
Facsimile: (310) 201-9160
E-mail: jcrowell@glancylaw.com

Lead counsel

BRONSTEIN, GEWIRTZ & GROSSMAN, LLC
Peretz Bronstein
60 East 42nd Street, Suite 4600
New York, NY 10165
Telephone: (212) 697-6484
Facsimile (212) 697-7296
Email: peretz@bgandg.com

Additional counsel

CERTIFICATE OF SERVICE

I hereby certify that on February 2, 2018, a copy of the foregoing was filed electronically via the Court's CM/ECF system and served by mail on anyone unable to accept electronic filing as indicated on the Notice of Electronic Filing. Notice of this filing will be sent by e-mail to all parties by operation of the Court's electronic filing system. I hereby certify that I caused to be mailed the foregoing document or paper via the United States Postal Service to the non-CM/ECF participants indicated on the Court's Manual Notice List. Parties may access this filing through the Court's CM/ECF System.

/s/ Jeremy A. Lieberman
Jeremy A. Lieberman