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

Ariana J. Tadler (*Pro Hac Vice*)
ATadler@TadlerLaw.com
TADLER LAW, LLP
One Penn Plaza
New York, New York
T: 212-946-9453
F: 212-273-4375

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

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

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

Attorneys for Plaintiffs and the Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

IN RE: YAHOO! INC. CUSTOMER DATA SECURITY BREACH LITIGATION	CASE NO. 16-MD-02752-LHK **SECOND AMENDED CONSOLIDATED CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

TABLE OF CONTENTS

For their Second Amended Consolidated Class Action Complaint, Plaintiffs Kimberly Heines, Hashmatullah Essar, Paul Dugas, Matthew Ridolfo, Deana Ridolfo, Yaniv Rivlin, Mali Granot, Brian Neff, and Andrew J. Mortensen, on behalf of themselves and all others similarly situated, allege the following against Defendant Yahoo! Inc. ("Yahoo"),[1] and Plaintiff Brian Neff, on behalf of himself and all others similarly situated, alleges the following against Defendants Yahoo and Aabaco Small Business, LLC ("Aabaco") (collectively with Yahoo, "Defendants"), based on personal knowledge as to Plaintiffs and Plaintiffs' own acts and on information and belief as to all other matters based upon, *inter alia*, the investigation conducted by and through Plaintiffs' undersigned counsel:

SUMMARY OF THE CASE

1. Giant information service providers such as Google, Facebook, Microsoft, and Yahoo experience a consistent stream of attacks on their data security. Quickly identifying and documenting those attacks, stopping them, and crafting better security measures to prevent them in the future is a normal, expected part of the business – except in Yahoo's case. Inexplicably turning a blind eye to this key aspect of its business, Yahoo did not just ignore security holes, it failed to set up the systems necessary to even detect or document them. This practice was long-term. Yahoo's own documents demonstrate that for nearly the last decade, Yahoo's systems have been breached again and again and again and that Yahoo in essence did nothing to protect its user data.

2. As a telling example, law enforcement notified Yahoo of a potential breach in late 2011. It took Yahoo until January 30, 2012, to retain an outside cybersecurity firm,

[1] In June, 2017, Yahoo's operating business was acquired by Verizon Communications Inc. ("Verizon"), with Yahoo continuing to exist as a wholly-owned subsidiary of Oath, Inc., a subsidiary of Verizon. In the event Yahoo is unable to satisfy any judgment entered in this case against it, and a successor entity is the proper defendant, plaintiffs will promptly move under Rule 25(c) to substitute Yahoo's successor as a proper defendant, which may be done at any time, including after judgment. *See Fed. Ins. Co. v. Laney*, No. C 12-04708 WHA, 2013 WL 3597309, at *2 (N.D. Cal. July 12, 2013) (noting that "Rule 25(c) has no time limit*."); Zest IP Holdings, LLC v. Implant Direct Mfg, LLC*, No. 10CV0541-GPC-WVG, 2013 WL 1626111, at *2 (S.D. Cal. Apr. 15, 2013) ("Rule 25(c) does not have a time limit, however, and joinder may occur at any point during litigation, even after judgment has been rendered.").

Mandiant, to investigate that breach. Even then, Yahoo did not want to investigate too thoroughly, instructing Mandiant not to perform any "Live Response or forensic analysis of any compromised system."

3. Even with the investigative limitations, Mandiant's resulting report, released to Yahoo in April 2012, was telling: the Report showed that in January to April 2012 at least two different potential nation state groups were able to access Yahoo's internal systems. Although the Report did not indicate that user credentials, email accounts or the contents of emails were targeted or taken, the fact that malicious actors were successfully infiltrating Yahoo's systems should have caused Yahoo to start to invest in greater security, event logging, monitoring, and improving the security of all internal and external user accounts. But, Yahoo did not. Collectively, these January to April 2012 incidents described in the Mandiant Report will be referred to as the "2012 Intrusions."

4. Yahoo's sheer recklessness with respect to data security led to predictable results. In September 2016, Yahoo rocked the technology world by disclosing that information was stolen from 500 million user accounts *two years earlier* in the then-largest known data breach in history (the "2014 Breach"). Only two months later, Yahoo again made headlines around the globe when it admitted to an even more massive breach—affecting upwards of 1 billion user accounts—that had occurred *three years* before Yahoo made the admission (the "2013 Breach").

5. In late 2017, the other shoe dropped. Yahoo admitted the 2013 Breach was even larger than originally disclosed—by a magnitude of three. *All three billion* Yahoo accounts then existing were breached in 2013, a fact that Yahoo falsely claims—as detailed herein—took more than four years to discover and disclose.

6. Yahoo's substandard security also permitted third parties to forge cookies, affecting approximately 32 million accounts between 2015 and 2016. Yahoo acknowledged the existence of the Forged Cookie Breach as early as November 2016, buried in the fine print of an SEC filing, but delayed notifying affected consumers for several months. In fact, Yahoo waited until a few months into 2017 to begin notifying Yahoo users that they had

been the victims of the "Forged Cookie Breach."[2]

7. During the 2013 and 2014 Breaches, hackers were able to take the names, email addresses, telephone numbers, birth dates, passwords, and security (Challenge / Response) questions of Yahoo account holders. As a result, the hackers gained access to the contents of *all* breached Yahoo accounts and, thus, any private information contained within users' emails, calendars, and contacts, including financial communications and records containing credit cards, retail accounts, banking, account passwords, IRS documents, and social security numbers from transactions conducted by email, in addition to other confidential and sensitive information. This compromised data is collectively referred to herein as "Personal Identifying Information" or "PII."

8. Despite the staggering magnitude of these breaches, Yahoo initially claimed that it did not discover the 2014 Breach or 2013 Breach *until 2016*. However, Yahoo's own internal documents clearly indicate that this claim was and is untrue. In fact, Yahoo—including key members of its legal team— knew about the 2014 Breach, internal code name "Siberia," *at the time it was occurring*. In an exchange on *November 5, 2014*, Yahoo personnel (Jeff Zingler, Software Development Engineer, and Andrew Rios, Incident Response) discuss a meeting with the legal team about the 2014 Breach:

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……

9. Indeed, although Yahoo's decision-makers made a conscious and deliberate decision not to alert any of Yahoo's customers that their PII had been stolen, they created a "reactionary" press release about the 2014 Breach, to use in the event that it became public

[2] The 2012 Intrusions, 2013 Breach, 2014 Breach, and Forged Cookie Breach are collectively referred to as the "Yahoo Data Breaches" or "Data Breaches."

before Yahoo wanted to disclose it.

10. In its 2016 annual filing with the SEC, Yahoo admitted an independent investigation showed it had "contemporaneous knowledge" of the 2014 Breach, yet failed to "properly investigate[] and analyze[]" the breach, due in part to "failures in communication, management, inquiry and internal reporting" that led to a "lack of proper comprehension and handling" of the 2014 Breach.[3] The 10-K provided additional details regarding Yahoo's failures:

> Specifically, as of December 2014, the information security team understood that the attacker had exfiltrated copies of user database backup files containing the personal data of Yahoo users but it is unclear whether and to what extent such evidence of exfiltration was effectively communicated and understood outside the information security team. However, the Independent Committee did not conclude that there was an intentional suppression of relevant information.
>
> Nonetheless, the Committee found that the relevant legal team had sufficient information to warrant substantial further inquiry in 2014, and they did not sufficiently pursue it. As a result, the 2014 Security Incident was not properly investigated and analyzed at the time, and the Company was not adequately advised with respect to the legal and business risks associated with the 2014 Security Incident. The Independent Committee found that failures in communication, management, inquiry and internal reporting contributed to the lack of proper comprehension and handling of the 2014 Security Incident. The Independent Committee also found that the Audit and Finance Committee and the full Board were not adequately informed of the full severity, risks, and potential impacts of the 2014 Security Incident and related matters. [4]

11. Even more astoundingly, Yahoo did not begin to disclose the 2013 Breach—the one involving all 3 billion accounts—until three years after it happened. Despite the wealth of evidence of ongoing security breaches and problems, Yahoo claims to have been totally unaware of this breach until being notified by law enforcement in 2016. Even after that, it took nearly another full year for Yahoo to disclose the true extent of the 2013 Breach, tripling its size.

---

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

[4] *Id*.

12. Restated in simple terms, Yahoo is claiming that in 2013 its data security measures and breach detection measures were so poor that hackers were able to access every single Yahoo account—roughly 3 billion—and exfiltrate users' PII, and Yahoo never detected it. This is the biggest data breach in history, by far, and Yahoo purports to have known nothing about it until told by someone else. Someone who, unlike Yahoo, was not charged with protecting Yahoo's stored information.

13. To make matters worse, at the time of the 2012 Intrusions and 2013 Breach, Yahoo was still using an encryption technology called MD5, which at least five years earlier had been publicly discredited and deemed "cryptographically broken and unsuitable for further use."[5] So, identity thieves had three full years of unfettered access to the inadequately-encrypted PII of roughly 3 billion user accounts before Yahoo even began to notify its users that their PII had been compromised.

14. Both the scope of these massive data breaches and Yahoo's baffling and unlawful delay in notification is unprecedented in the information technology world.

15. This Second Amended Consolidated Class Action Complaint is filed on behalf of all persons in the United States and Israel, described more fully in the following sections, whose PII was compromised in the 2012, 2013, 2014, or Forged Cookie Breaches. The class representatives here have suffered actual harm, including, but not limited to, having false tax returns filed in their name, having credit card accounts fraudulently opened in their names, having fraudulent charges posted to their credit cards and bank accounts, having their government benefits stolen, and having spam and phishing emails sent constantly from their Yahoo addresses. The compromise of the Class members' PII has also caused the Class members to pay for credit monitoring, account freezes, card and account replacements, and late fees for delayed payments. Class members have devoted and will continue to devote time and energy to recovering stolen funds (where possible), tracking and repairing damage to

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

their credit reports and reputations, and monitoring and protecting their accounts. Plaintiffs and Class members are further damaged as their PII remains in Defendants' possession, without adequate protection, and is also in the hands of those who obtained it for its commercial value, without Plaintiffs' or Class members' consent. Further, members of the Small Business Class and the Paid Users Class have lost the benefit of their bargain and purchased services they otherwise would not have, or paid more for supposedly secure services than they would have, had they known the truth regarding Defendants' inadequate data security.

JURISDICTION AND VENUE

16. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, there are more than 100 class members, and at least one class member is a citizen of a state different from Defendants and is a citizen of a foreign state. The Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

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

PARTIES

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

18. Plaintiff Kimberly Heines is a resident and citizen of Magalia, California. Ms. Heines receives approximately $1,100 per month from Social Security Disability to meet her

essential needs, including food and housing. Plaintiff Heines opened a Yahoo account nearly twenty years ago and used it for all of her online communications, including communications relating to her education, financial aid, employment, banking, healthcare, and personal finances. Plaintiff Heines' Yahoo emails included PII and information relating to her account with Direct Express, the payment service through which she receives her Social Security Disability benefits. On February 4, 2015, Plaintiff Heines discovered that her entire monthly disability allowance had been stolen from her Direct Express account and used to purchase gift cards at Rite Aid (in the amounts of $513.58 and $507.10), and Walgreens (in the amount of $118.00). Plaintiff Heines had her Direct Express card in her possession at the time of the thefts and was away from home caring for a hospitalized relative, more than 600 miles from where the thefts occurred. Because she had no other source of income, the theft put her in an extremely vulnerable and stressful situation in which she literally had to rely on the kindness of strangers to survive for two weeks. Plaintiff Heines is normally very conscientious about paying bills on time but the theft caused her to pay her rent and some utility bills late, which resulted in late fees of more than $30. Soon after the theft, Ms. Heines started receiving collection calls regarding debts she had not incurred. She also saw unfamiliar debts appearing on her credit report and her credit score suffered as a result. Plaintiff Heines filed a police report and spent over 40 hours talking to the police, the Social Security Administration, Direct Express, RiteAid, Walgreens, and others to have the funds restored to her Direct Express account and deal with other consequences of the data breach, the resulting theft, and the consequences of the theft. In or about September 2016, Plaintiff Heines received an email notice from Yahoo informing her that her Yahoo accounts and PII may have been compromised in the 2014 Breach. In addition to the damages detailed herein, the Yahoo Data Breaches have caused Plaintiff Heines to be at substantial risk for further identity theft.

19. Plaintiff Hashmatullah Essar is a resident and citizen of Thornton, Colorado. Mr. Essar is a retail manager for a local bank and handles retail and banking accounts. Approximately 15 years ago, Mr. Essar opened two email accounts with Yahoo. Mr. Essar

carefully read the Terms of Service before opening his email accounts and would not have opened them if he had any concerns about the security of Yahoo email. Mr. Essar used his Yahoo email accounts for all of his personal, financial, and business needs. More specifically, Plaintiff Essar transacted business, shopped online, sent personal messages, communicated with his accountant, received bank account statements, applied for jobs, secured a mortgage for his home, and refinanced that mortgage, through his Yahoo e-mail account. Plaintiff Essar first became concerned about the security of his Yahoo email accounts when he received phishing emails from a credit card company purporting to be affiliated with American Express, asking him to follow a link to log-in to his "Serve" account. Plaintiff Essar knew the email to be false because he did not have a "Serve" account through American Express. Subsequently, in October 2016, Mr. Essar received an email notice from Yahoo notifying him of the 2014 Breach, and informing him that his Yahoo accounts and PII may have been compromised. As a result of the breach notification, and concerned for his own and his family's well-being, Plaintiff Essar signed up for a credit counseling class through his employer to learn how to limit, recognize, and respond to identity theft. In addition, as a direct result of the 2014 Breach, Mr. Essar signed up for and paid (and continues to pay) $35.98 per month for LifeLock credit monitoring service. Notwithstanding his attempts to limit the damage done to his credit and identity as a result of the 2014 Breach, Mr. Essar has suffered great harm as a result of the Breach. Plaintiff Essar not only lost years of email messages when several hundred simply vanished from his Yahoo account, he also experienced tax fraud in February 2017, when an unauthorized person fraudulently filed a tax return under his Social Security Number. Further, Mr. Essar was denied credit in March 2017 due to the identity theft he suffered as a result of the 2014 Breach, and freezes were placed on his credit. Because Plaintiff Essar is a United States citizen of Afghani descent, he worries that a terrorist sympathizer may steal his PII and may use it to commit crimes in his name, so much so that he suffers from extreme anxiety and has difficulty sleeping. Finally, the Yahoo Data Breaches have caused Plaintiff Essar to be at substantial risk for further identity theft.

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

21. Plaintiffs Matthew and Deana Ridolfo are a married couple and residents and citizens of Vineland, New Jersey. Plaintiff Deanna Ridolfo works with a public school system and Plaintiff Matthew Ridolfo is a mechanical designer for a local company. Both Plaintiffs used their Yahoo accounts for nearly twenty years for general banking, credit card management and communications, a mortgage refinance, and communication with friends and family. In June 2016, Plaintiff Matthew Ridolfo used his Yahoo email account to send scanned copies of sensitive financial documents in order to refinance the couple's home mortgage. Shortly thereafter, in December 2016, both Mr. and Mrs. Ridolfo received notice

of the 2013 Breach. On January 4, 2017, Plaintiff Deana Ridolfo received a letter from Citibank informing her that Citibank was concerned that her Citibank card was fraudulently accessed. Since Plaintiff Deana Ridolfo had never opened a Citibank account, she immediately knew it was a fraudulent card. Mrs. Ridolfo contacted Citibank immediately and learned that cash advances and Uber charges were listed on the account that had been opened in her name. Citibank also informed her that a second Citibank account was recently applied for in her name, this one for a Sears branded credit card. As a result of the letter and information received from Citibank, the Ridolfos immediately obtained free credit reports through Experian. Plaintiff Deana Ridolfo learned that someone attempted to open an account at Barclay Bank, two accounts at Lowes, and a Walmart account in her name. Further, Mrs. Ridolfo learned that an American Express account was fraudulently opened in her name, and $900.00 had been charged on a fraudulently opened Target credit card. Mr. Ridolfo learned that a total of eleven credit card or bank accounts had been fraudulently opened or attempted to be opened during the month of December 2016 in his name through the following retailers and banks: Brooks Brothers, Brandsource, Citi Doublecash, Capital One, Walmart, Lowes, Sears Mastercard, TD Bank, Barclays Bank of Delaware, Santander Bank, and Banco Popular of Puerto Rico. In addition, fraudulent addresses were listed for the Ridolfos in Florida and Virginia. As a result of this significant fraud, both Plaintiffs Matthew and Deana Ridolfo were forced to individually call each bank to report the fraudulent accounts and charges, spending significant time talking with credit card fraud departments.

22. Further, unauthorized persons hacked into the Ridolfos' personal home phone line through Comcast and forwarded their home line phone calls to an unknown phone number. Plaintiffs Matthew and Deana Ridolfo made countless phone calls to credit card companies, Experian, TransUnion, Equifax, Innovis, the Internal Revenue Department, the Department of Motor Vehicles, and the Social Security Administration to help protect their sensitive and confidential information. Further, the Ridolfos were forced to file police reports in New Jersey, Florida and Virginia to protect their identity. In addition, Plaintiffs Matthew and Deana Ridolfo purchased and enrolled in LifeLock to have help monitoring their credit

and finances, expending approximately $30.00 per month each for a total of over $60.00 per month. Despite enrolling in a credit monitoring program, placing freezes on their credit, and individually notifying credit card companies and banks, an unauthorized person attempted to open another credit card account on January 31, 2017 in Plaintiff Deana Ridolfo's name. On June 26, 2017, Deana and Matthew Ridolfo were contacted by the Miami-Dade State Attorney's Office regarding the arrest of a parolee whom police later found to be in possession of a "journal" containing a list of approximately 200 names with additional personal identifying information next to each name. Among those listed, according to the State Attorney's Office, were Matthew and Deana Ridolfo. Next to Matthew's name was his Yahoo email address and Yahoo account password (used up until Yahoo prompted a password change following the breach announcements) as well as the Sears credit card number fraudulently opened in Mr. Ridolfo's name. Next to Deana's name was the Citibank credit card number also fraudulently opened in her name. Finally, the Yahoo Data Breaches have caused Plaintiffs Matthew and Deana Ridolfo to be at substantial risk for further identity theft.

B. Class Representatives for the Israel Class

23. Plaintiff Yaniv Rivlin is a resident of Tel Aviv, Israel, and has dual Israeli and Canadian citizenship. Plaintiff Rivlin opened his Yahoo email account in Israel approximately ten years ago mainly for personal purposes, including banking, friends and family, credit card statements, and social security administration. Plaintiff Rivlin pays Yahoo annually $20.00 to have Yahoo emails received forwarded to another email account. Plaintiff Rivlin maintains a credit card on file with Yahoo to pay for the forwarding service. Plaintiff Rivlin was notified by Yahoo on December 20, 2016 that his Yahoo email account had been breached. After the notification, Plaintiff Rivlin noticed an increase in unsolicited emails, including spam and advertisements. Plaintiff Rivlin also spent, and continues to spend, time and effort proactively changing username and passwords on many of his accounts to prevent fraud. In addition, the Yahoo Data Breaches have caused Plaintiff Rivlin to be at substantial risk for identity theft, if in fact his identity has not already been stolen.

24. Plaintiff Mali Granot is a resident and citizen of Raanana, Israel. Plaintiff Granot maintained a Yahoo email account, which she opened in Israel in the fall of 1998, for personal reasons, specifically to correspond with family, friends, and school. Plaintiff Granot was unexpectedly locked out of her Yahoo email account and unable to gain access. Plaintiff Granot eventually gained access to her Yahoo email account by answering security questions. However, once she opened her Yahoo email account, she received unsolicited pop-up chat requests and other unsolicited requests including for services that she had not requested but that someone had requested in her name using her Yahoo email account. In addition, the Yahoo Data Breaches have caused Plaintiff Granot to be at substantial risk for identity theft, if in fact her identity has not already been stolen.

C. Class Representative for the Small Business Users Class

25. Plaintiff Brian Neff is a citizen and resident of Texas. In September 2009, in connection with his online insurance agency business, he contracted with Yahoo for two services, Yahoo! Web Hosting for www.TheInsuranceSuite.com and Yahoo! Business Email, for which he paid Yahoo $13.94 every month from September 2009 through approximately June 2017. Before contracting with Yahoo for these services, Mr. Neff read the applicable Terms of Service and the website content regarding those services thoroughly and carefully and relied upon, among other provisions, Yahoo's contractual commitments and representations that his PII would be secure. Between 2009 and the present, at various times, Plaintiff Neff used Defendants' web hosting services in connection with another 54 websites, paying anywhere from $3.94 to $15.94 per month for each website. Prior to contracting with Yahoo or Aabaco for each of these websites, Mr. Neff reviewed the Terms of Service and website content for major changes, and each time he relied upon Yahoo's or Aabaco's contractual commitments and representations that his PII would be secure. In addition, every time Yahoo or Aabaco made changes to the Terms of Service and notified him of same, Mr. Neff carefully reviewed the changes, and each time he relied upon Yahoo's or Aabaco's contractual commitments and representations that his PII would be secure.

26. On December 14, 2016, Plaintiff Neff received a notice from Yahoo informing him that hackers had stolen account information that he had provided to Defendants—information that "may have included names, email addresses, telephone numbers, dates of birth, hashed passwords [using outdated encryption] and, in some cases, encrypted or unencrypted security questions and answers." In addition to losing the benefit of his bargain by paying, and overpaying, Yahoo thousands of dollars for services that subjected him to security breaches (damaging him in the full amount of those payments), Plaintiff Neff was also a victim of actual identity theft, which, upon information and belief, was caused by one or more of the Yahoo Data Breaches. In May 2015, Plaintiff Neff incurred fraudulent charges on his Capital One credit card and his Chase debit card, both of which were on file with Yahoo to pay for services connected with two of his websites, with Yahoo being the only company to which Plaintiff Neff had provided information about both accounts. In addition to these fraudulent charges, also in May 2015, an unauthorized credit card account in Plaintiff Neff's name was opened at Credit One Bank, and unauthorized and fraudulent charges were made to that account in May and June 2015. Plaintiff Neff had to spend significant time and incurred expenses mitigating the harm to him from these security breaches and identity theft. As to both the Capital One and Chase cards, Plaintiff Neff had to make several phone calls to each to notify them of the fraudulent charges and to have the accounts frozen. Plaintiff Neff had to change passwords for both cards and he then had to wait two to four days to receive new cards from each. As to the Credit One Bank credit card opened in his name, Plaintiff Neff had to call the police department and file a police report, fill out an FTC affidavit, engage in multiple phone calls to Credit One over several weeks totaling multiple hours, and put together a package of materials for Credit One, which took hours, and which he sent to Credit One via Federal Express overnight delivery at a cost of $11.87. In addition, at a time when Plaintiff Neff was trying to pre-qualify for a home mortgage, he learned that his credit reports contained negative information about over-limits and unpaid charges on the fraudulent Credit One Bank credit card. He had to write a demand letter to Credit One Bank to force it to contact Experian and TransUnion and have these

negative items removed from his credit reports. Mr. Neff has never been notified that he was a victim of any other data breach.

27. Since these incidents, Plaintiff Neff has been reviewing reports from complimentary credit monitoring offered by all his credit cards which offer that complimentary service, reviewing daily updates from Credit Karma, and he has ordered and reviewed free annual reports from all three credit bureaus—all activities to which he has been required to devote many hours of time. Since he became aware of the inadequacy of Defendants' online security, Plaintiff Neff stopped using the TheInsuranceSuite.com website, costing him many valuable leads, in the range of 2,500–3,000, for his insurance business. Further, Plaintiff Neff is in the process of migrating that website to a more secure provider. The cost to transfer Plaintiff Neff's accounts and services currently with Defendants to a company with adequate security will be in excess of $10,000, due to the nature and capacity of his website and the cost to reestablish the high search engine placement he had earned over the last eight years, among other factors. Finally, the Yahoo Data Breaches have caused Plaintiff Neff to be at substantial risk for further identity theft.

D. Class Representative for the Paid Users Class

28. Plaintiff Andrew J. Mortensen is a resident and citizen of Dallas, Texas. Plaintiff Mortensen was a New Jersey, Oklahoma, and then Texas resident during the pendency of the 2013, 2014 and Forged Cookie Data Breaches. Plaintiff Mortensen has been a Texas resident since May 2014. Plaintiff Mortensen opened a Yahoo email account in or around 2004, has paid Yahoo for services since 2007, and has used his email account for both personal and business purposes. Plaintiff Mortensen has paid $19.95 per year for Yahoo's premium email service since December 2007. Plaintiff Mortensen received banking, credit card, investment account, business emails, personal emails, bill pay information, medical, and automobile information in his Yahoo account. Plaintiff Mortensen regularly used his Yahoo email account to monitor and/or manage banking information, financial information, and online bill payments, as well as to communicate and share personal information with family and friends. Plaintiff Mortensen has experienced increased suspicious phone calls or

emails, including spam calls once a week, and spam texts every two weeks. As a result of the Data Breaches, Plaintiff Mortensen was forced to expend approximately three hours of time and effort checking credit and opening accounts (and will be forced to expend additional time in the future), and has experienced anxiety as a result of the Data Breaches. Yahoo's failure to timely and adequately notify its accountholders of the 2014 Data Breach put Plaintiff Mortensen at greater risk of identity theft and other fraud. In or about December 2016, Plaintiff Mortensen received notice from defendant Yahoo that his PII had been compromised due to a data breach. Plaintiff Mortensen was not notified by Yahoo without unreasonable delay, and was injured as a result.

E. Defendants

29. Yahoo is a Delaware corporation registered with the California Secretary of State, with its principal place of business and headquarters in Sunnyvale, California, located at 701 First Ave., Sunnyvale, CA 94089. In June, 2017, Yahoo, Inc. completed the sale of substantially all of its assets to Verizon. Yahoo continues to exist as a wholly-owned subsidiary of Oath, Inc., a subsidiary of Verizon. The remaining assets of Yahoo, Inc. were renamed Altaba.[6]

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

31. At all relevant times, Aabaco has been the alter ego of Yahoo for its small business subscribers and has been wholly owned and managed by Yahoo. Yahoo and Aabaco

[6] *See* fn. 1.

are also joint venturers and are jointly responsible to small business customers for any wrongful acts carried out by Aabaco that are material to this suit. Finally, Aabaco is the successor in interest to the Yahoo Small Business division and is liable to small business customers, in addition to Yahoo, as the successor for any wrongdoing by that division before it was renamed Aabaco.

FACTUAL BACKGROUND

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

32. One of the web's earliest pioneers, Yahoo was founded in 1994 as a directory of websites, but quickly developed into a source for searches, email, shopping, and news. Currently, its services attract at least one billion visitors per month. Yahoo sister sites include Flickr, Yahoo Finance, and Yahoo Fantasy Sports, among others.

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

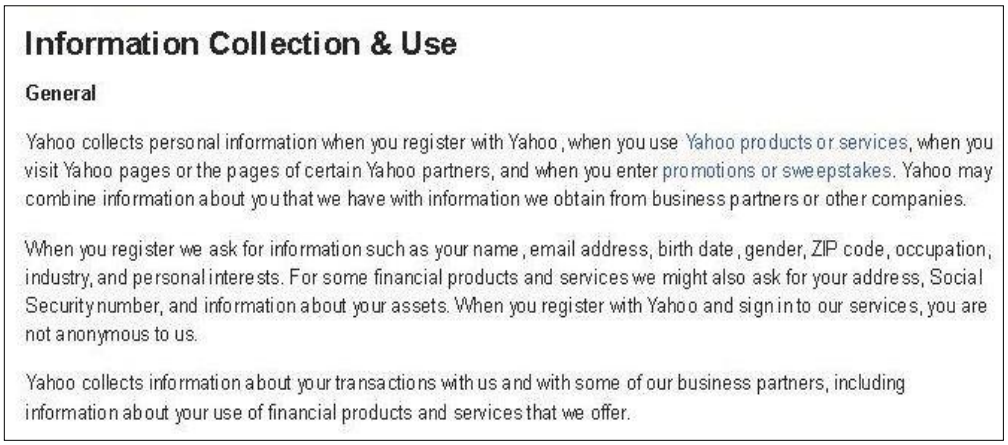
34. Yahoo also offers various online services to small businesses. Popular services include website hosting, which makes it easy for businesses to create and operate a business website, advertising for those businesses, and email services for communications between businesses and their customers. To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

35. When users establish any of the above accounts with Defendants, users must provide Defendants with PII, which Defendants then electronically collect, store on, and

route through its U.S.-based servers, a majority of which are located in California. And, in fact, Plaintiffs and Class members signed up for online Yahoo accounts and provided the required PII, including, in some cases, debit and credit card information, which, Defendants collected, stored, and routed through its U.S.-based servers.

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

37. The "Privacy Center" portion of Yahoo's website delineates the type of personal information it collects directly from its account holders.[7] Yahoo's Privacy Policy, which is incorporated by reference into the Terms of Service to which all users must agree when they create their accounts, explains[8]:



Information Collection & Use

General

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

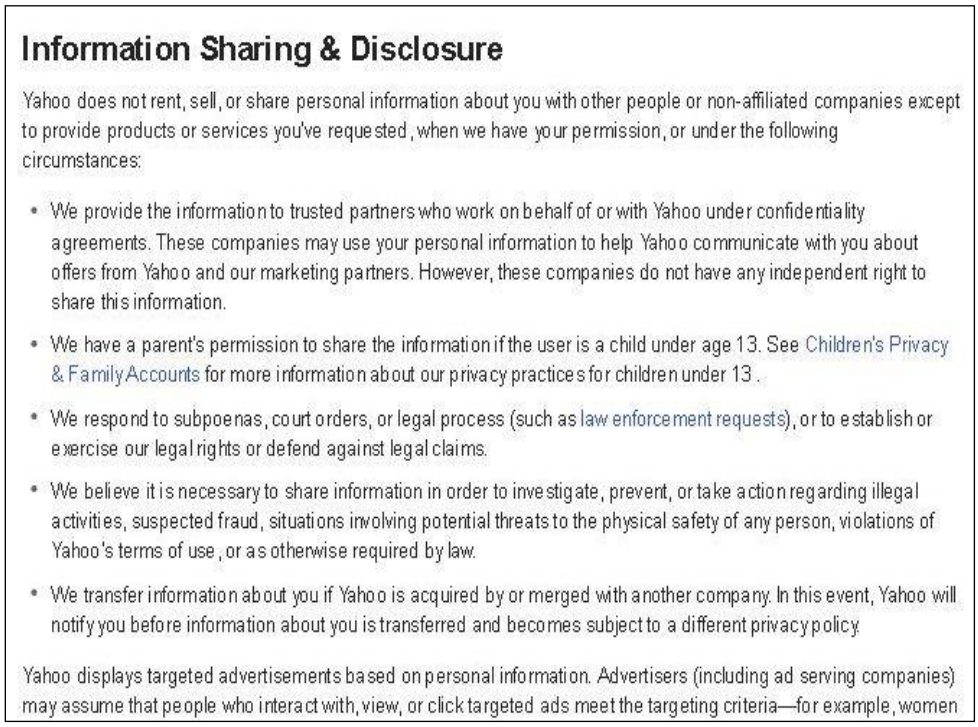
When you register we ask for information such as your name, email address, birth date, gender, ZIP code, occupation, industry, and personal interests. For some financial products and services we might also ask for your address, Social Security number, and information about your assets. When you register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

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

[7] Yahoo Privacy Center, Yahoo!, https://policies.yahoo.com/us/en/yahoo/privacy/index.htm (last visited Apr. 5, 2017).

[8] Yahoo's Terms of Service for the years 2011-2016 are attached to this First Amended Consolidated Class Action Complaint as Exhibits 1 through 6, respectively. Yahoo's Privacy Policies for those same years are attached as Exhibits 7-12, respectively.

38. Yahoo also informs its account holders that it shares personal information provided by account registrants only under limited circumstances.[9]



Information Sharing & Disclosure

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

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

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

39. Each time Yahoo made changes to its Terms of Service, Plaintiffs and the members of the Class were required to accept the new Terms by way of a clickwrap agreement. Plaintiffs who did not accept the new Terms of Service would not be able to continue to use their Yahoo accounts.

40. At all times relevant herein, Yahoo represented and warranted to Plaintiffs and the Class members that its databases containing PII were secure and that customers' PII would remain private.

41. Yahoo made promises to Class members in its Privacy Policies, including[10]:

> 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.

[9] *Id.*

[10] *See, e.g.*, Exh. 9, Yahoo! Privacy Policy – 2013.

42. In 2016, Yahoo updated its Privacy Policy to clarify the protections it provided in connection with data transfer[11]:

> **Data Transfer**
>
> Your personal information may be transferred to countries other than your own to process and store data in accordance with our Privacy Policy and to provide you with products and services. Some of these countries may not have the same data protection safeguards as the country where you reside. By using our products and services, you consent to us transferring your data to these countries. We are committed to ensuring your information is protected and apply safeguards in accordance with applicable law.

43. Yahoo made further guarantees on its "Security at Yahoo" page (hyperlinked from Yahoo's Privacy Policy)[12]:

> **Security at Yahoo**
>
> Protecting our systems and our users' information is paramount to ensuring Yahoo users enjoy a secure user experience and maintaining our users' trust. We have taken the following measures to protect your information:
>
> Secure Storage
> We deploy industry standard physical, technical, and procedural safeguards that comply with relevant regulations to protect your personal information.

44. None of these representations were true.

B. Yahoo's Small Business Customers Depended on Defendants' PII Security Practices

45. Defendants Yahoo and Aabaco understand that online security is paramount to their Small Business customers and was and is highly material to their decision to use Defendants' Small Business services. Defendants address these concerns in the advertising that Defendants present to all would-be customers exploring the Small Business services. All customers, including Plaintiff Neff, were exposed to and read these advertisements and explanations, which appear on the webpages all customers must use to sign-up for the services.

46. Defendants made similar representations about the importance of security on Aabaco's website as they did for Yahoo's main page: "We have physical, electronic, and

[11] Exh. 12, Yahoo! Privacy Policy – 2016.

[12] Security at Yahoo, Yahoo!, https://policies.yahoo.com/us/en/yahoo/privacy/topics/security/index.htm (Attached as Exhibit 13). The current version of the "Security at Yahoo" page is attached as Exhibit 14.

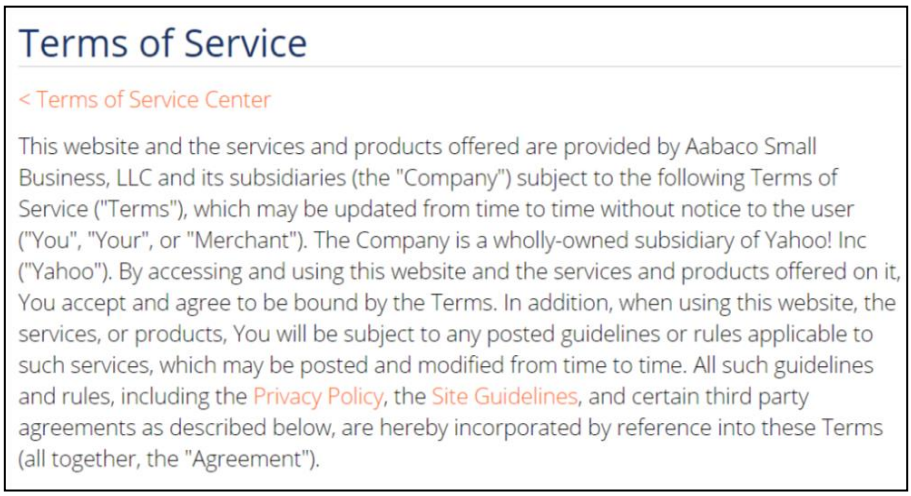
procedural safeguards that comply with federal regulations to protect your Personal Information."[13] This page is attached to this First Amended Consolidated Class Action Complaint as Exhibit 15.

47. For example, the current web hosting advertisement and explanations page assures that web hosting is safe and secure[14]:

48. The relationship between Defendants and Small Business Class Members is governed by Defendants' Terms of Service, which incorporate by reference a number of other agreements including Defendants' Privacy Policy ("Privacy Policy"). Throughout the relevant time, the Terms of Service was a "click-through" agreement. Each member of the Small Business Users Class, including Plaintiff Neff, prior to becoming a Small Business customer, was required to click a box stating that "I agree to the terms of service," with terms of service being a live link page that would open when clicked.[15]

[13] Privacy Policy, Yahoo! Aabaco Small Business, https://www.aabacosmallbusiness.com/privacy-policy (last visited Apr 9, 2017).
[14] Flexible hosting for your professional website, Yahoo! Aabaco Small Business, https://smallbusiness.yahoo.com/webhosting#reliable (last visited Apr. 12, 2017).
[15] Account Creation and Login Page, Yahoo! Aabaco Small Business, https://login.luminate.com/registration?.src=smbiz&.done=https%3A%2F%2F www.luminate.com (last visited Apr. 5, 2017).

49. The Terms of Service expressly refer to both Aabaco and Yahoo[16]:



Terms of Service

< Terms of Service Center

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

50. The Privacy Policy has been updated over the years but, as relevant to this action, has always contained identical or substantively similar assurances that Defendants appropriately safeguard the PII entrusted to them.[17] The Privacy Policy in effect throughout the relevant time represents that:

CONFIDENTIALITY AND SECURITY

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

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

[16] Terms of Service, Yahoo! Aabaco Small Business, https://smallbusiness.yahoo.com/tos (last visited Apr. 5, 2017).

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

51. In addition, the Privacy Policy represents that Defendants do not share PII except in the following delineated circumstances[18]:

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

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

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

C. PII is Very Valuable on the Black Market

54. The types of information compromised in the Yahoo Data Breaches are highly valuable to identity thieves. In addition to credit and debit card information, names, email addresses, recovery email accounts, telephone numbers, birthdates, passwords and security

[18] *Id.*

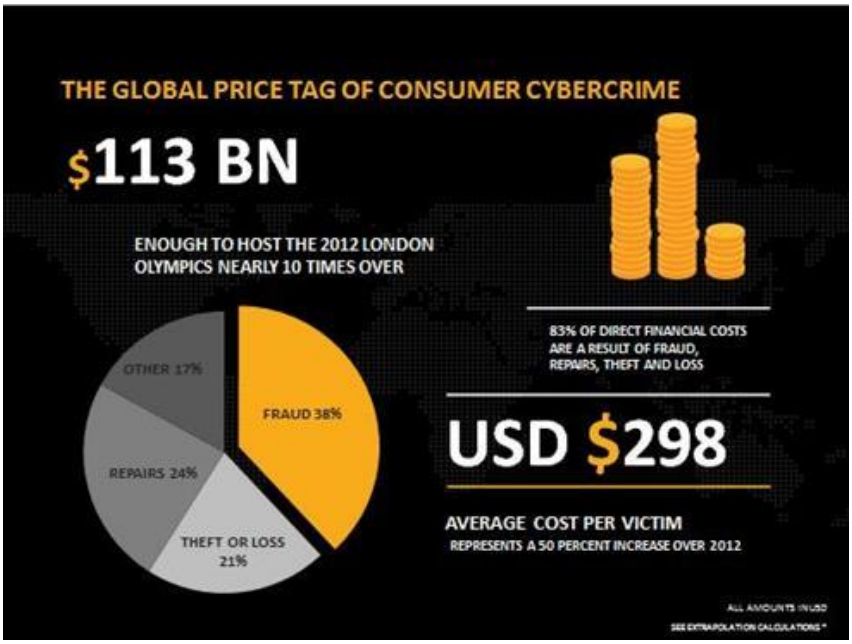
question answers can all be used to gain access to a variety of existing accounts and websites. Indeed, Plaintiffs and Class members have suffered a variety of consequences from the breaches, including forged credit applications, the opening of unauthorized credit card accounts, fake tax returns being filed under their names, fraudulent charges, email hacks, unauthorized access to payment accounts such as PayPal and Western Union, gift cards being generated from their accounts without their consent, and numerous other identity theft-related damages.

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

> In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.[19]

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

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



57. The problems associated with identity theft are exacerbated by the fact that many identity thieves will wait years before attempting to use the PII they have obtained. Indeed, in order to protect themselves, Class members will need to remain vigilant against unauthorized data use for years and decades to come.

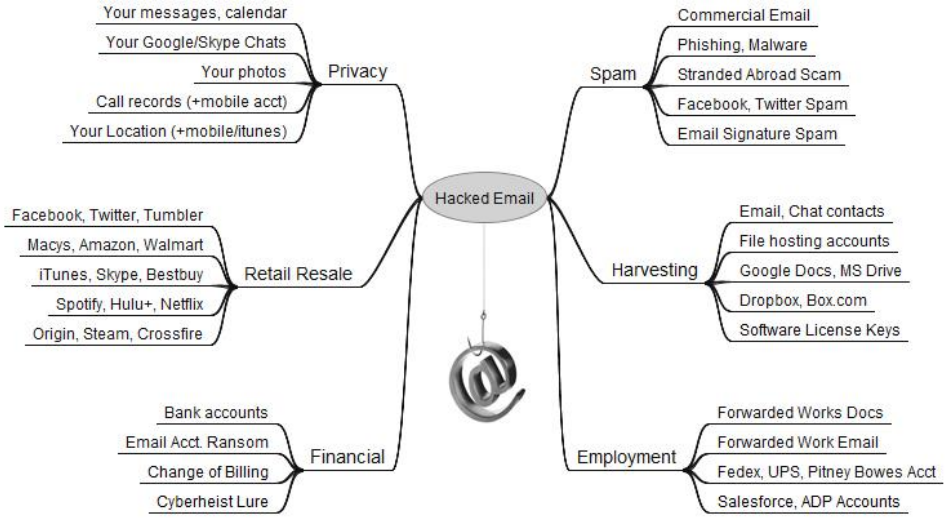
58. Once stolen, PII can be used in a number of different ways. One of the most common is that it is offered for sale on the "dark web," a heavily encrypted part of the Internet that makes it difficult for authorities to detect the location or owners of a website. The dark web is not indexed by normal search engines such as Google and is only accessible using a Tor browser (or similar tool), which aims to conceal users' identities and online activity. The dark web is notorious for hosting marketplaces selling illegal items such as weapons, drugs, and PII.[20] Websites appear and disappear quickly, making it a very dynamic environment.

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

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

60. In addition to PII, a hacked email account can be very valuable to cyber criminals. Since most online accounts require an email address not only as a username, but also as a way to verify accounts and reset passwords, a hacked email account could open up a number of other accounts to an attacker.[21]

61. As shown below, a hacked email account can be used to link to many other sources of information for an identity thief, including any purchase or account information found in the hacked email account.[22]



D. Yahoo Turns a Blind Eye to Gaping Holes in Its Security, Refusing to Upgrade After Repeated Intrusions and Negative Assessments

62. Yahoo has a storied, unfortunate history of inadequate and outdated data security. For at least the last decade and a half, Yahoo has been repeatedly put on notice that its security measures were not up to par, leaving users' PII at risk of theft. Rather than

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

[22] Brian Krebs, The Value of a Hacked Email Account, KrebsonSecurity (June 13, 2013, 3:14 PM), https://krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account/.

addressing the problems by upgrading its data security, Yahoo continued to use outdated security methods long after vulnerabilities were brought to Yahoo's attention. Yahoo's refusal to heed myriad warnings about its deficient data security, even after multiple breaches, created the environment that permitted unauthorized users to abscond with Plaintiffs and Class members' PII.

63. Yahoo's systems have been vulnerable to a wide variety of attack methods. In 2001, then-20-year-old hacker Adrian Lamo showed he could rewrite published articles on Yahoo! News without even having to enter a password.[23]

64. In 2008, multiple hosts on Yahoo's corporate network were compromised and attackers targeted [redacted]

65. In 2009, the [redacted] attacks continued; [redacted]

66. In 2010 alone, Google informed Yahoo that Yahoo 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 the 2008 access identified above; [redacted]

[23] Kevin Poulsen, Yahoo! News Hacked, SecurityFocus (Sept. 18, 2001), http://www.securityfocus.com/news/254.

67. In 2011, then- Chief Information Security Officer (CISO), a senior-level executive at Yahoo, Justin Somaini presented at a third quarter Information Risk Management All Hands meeting, identifying gaping holes in Yahoo's data security:

[redacted]

68. [redacted].

69. Also in 2011, Yahoo hired Ramses Martinez as the Senior Director of Threat Response. When he was hired, there were only 5 people on Yahoo's "Paranoids" team, the team charged with managing all data security incidents in a company of over 14,000 people and 100 properties.

70. With such major deficiencies, it was only a matter of time until a major intrusion occurred.

71. More than a month later, on January 30, 2012, Yahoo retained Mandiant to investigate and perform a Threat Assessment Program (TAP). Yahoo limited the assessment, instructing Mandiant to "not perform Live Response or forensic analysis of any compromised system."

72. On February 9, 2012, Mandiant conducted a two-hour training session on industry best practices for remediation activities. The following day, on the tenth, Yahoo conducted a "remediation event."

73. Less than a week later, on February 16, 2012, Yahoo was alerted by a third party that a vulnerability existed within its systems that allowed people to use a certain URL to crack Yahoo accounts—"they are able to try and crack as many accounts as they want."

74. Mandiant conducted its assessment between February 13 and April 3, 2012. In its subsequent report, dated April 20, 2012, Mandiant identified the earliest evidence of a related intruder on Yahoo's networks as March 22, 2010.

75. Mandiant found a number of Remote Access Trojans (RATs) deployed across Yahoo's systems. Depending on how they are built, RATs can give their operators access to virtually everything on a compromised system. RATs are a form of malware that can give an unauthorized third party the same access to a system as if the third party were physically at the terminal, and are often downloaded alongside a program or file requested by the authorized user, such as through a seemingly legitimate email attachment. During its assessment, Mandiant observed an attacker performing ***live intrusions into Yahoo's corporate network*** This was done through the earlier installation of a RAT into Yahoo's systems.

76. Mandiant detected at least two different attack groups in Yahoo's systems, with the most recent activity seen on April 1, 2012—meaning Yahoo's self-performed remediation efforts failed. Mandiant considered these attack groups to be Advanced Persistent Threats (APTs), a term used to describe a category of well-trained hackers believed to be state-sponsored.

77. Mandiant's report also identified 41 Yahoo systems with evidence of compromise, with an additional four potentially compromised systems.

78. While onsite, Mandiant actually displayed to Yahoo an active, ongoing attack on March 26, 2012.

79. Immediately following the Mandiant report and the "cleaning" of the limited in-scope systems identified in the Mandiant report, Yahoo stopped investigating and claimed they had successfully eliminated all threats on April 8, 2012. Within ten days later, a compromise of Yahoo's Citrix environment was uncovered.

80. Yahoo claimed to have eliminated the new system intrusions but waited until June of 2012 to hire Microsoft to investigate. .

81. Later in 2012, Yahoo admitted that more than 450,000 user accounts were compromised through an SQL injection attack—with the passwords simply stored in plain text. This breach revealed that Yahoo apparently had failed to take even basic precautions to protect its customers' data. Indeed, news outlets reported that "[s]ecurity experts were befuddled … as to why a company as large as Yahoo would fail to cryptographically store the passwords in its database. Instead, they were left in plain text, which means a hacker could easily read them."[24] This breach came to be known as the "D33D" breach, named after the hacker group behind it.

82. According to Marcus Carey, a security researcher at Rapid7, the D33D hack showed Yahoo was far behind the times. "It is definitely poor security. It's not even security 101. It's basic application development 101."[25] Indeed, the Federal Trade Commission considered SQL injection attacks a known—and preventable—threat as far back as 2003.[26]

83. The D33D hack was meant—and should have served—as a "wake up call" to Yahoo that it had inadequate protections for users' personal information.[27] In fact, a message purportedly left by the hackers on the webpage where the information was dumped claimed as much:

---

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

[25] *Id.*

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

[27] Plaintiffs are not alleging claims related to the 2012, D33D attack.

> 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.[28]

84. Yahoo should have immediately invested in security upgrades following the 2012 Intrusions, the associated Mandiant report, and the D33D attack.

85. Rather than increasing its security forces 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 CISO, Justin Somaini. Somaini reportedly left due to disagreements with CEO Marissa Mayer's management style. Yahoo left the position vacant for more than a year, until March 2014.

86. 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 chose to stick its proverbial head in the sand rather than fix the problems.

87. One recurrent problem Yahoo steadfastly refused to fix was the issue of inadequate logging standards. This inadequacy comes up again and again in the security reports prepared for Yahoo. Dell SecureWorks ("DSW"), which Yahoo engaged multiple times from 2013 through 2016, raised the issue with Yahoo repeatedly. During one such 2013 incident, internal code name "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.

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

[28] 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/.

89. [redacted].

90. [redacted]

[redacted]

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

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

[redacted]

93. Unfortunately, Yahoo's culture actively discouraged emphasis on data security. For example, former Yahoo security staffers interviewed later told Reuters that requests made by Yahoo's security team for new tools and features such as strengthened cryptography protections were, at times, rejected on the grounds that the requests would cost too much money, were too complicated, or were simply too low a priority.[29]

E. Yahoo's Inadequate Data Security Allows the Massive Breach of 3 Billion User Accounts in 2013, Which Yahoo Then Fails to Disclose

94. As an example of Yahoo's refusal to keep abreast of cybersecurity issues, in the summer of 2013, Yahoo decided to finally abandon the use of a discredited technology for encrypting data known as MD5. MD5 was well known as a weak password protection method by hackers and security experts for years before the 2013 Breach. MD5 can be cracked more easily than other so-called "hashing" algorithms, which are mathematical functions that convert data into seemingly random character strings.[30]

95. In fact, five years before Yahoo finally took action, Carnegie Mellon University's Software Engineering Institute issued a public warning to security professionals through a U.S. government-funded vulnerability alert system, stating that: MD5 "should be considered cryptographically broken and **unsuitable for further use**."[31]

96. "MD5 was considered dead long before 2013," said David Kennedy, chief executive of cyber firm TrustedSec. "Most companies were using more secure hashing algorithms by then."[32] Common techniques such as "salting" (adding a unique secret to the password) and "stretching" (repeating the hashing process over many times) hashed

---

[29] Reuters, Why Yahoo's Security Problems Are a Story of Too Little, Too Late, FORTUNE (Dec. 18, 2016), http://fortune.com/2016/12/19/yahoo-hack-cyber-security/.
[30] Reuters, Why Yahoo's Security Problems Are a Story of Too Little, Too Late, FORTUNE (Dec. 18, 2016), http://fortune.com/2016/12/19/yahoo-hack-cyber-security/.
[31] Vulnerability Note VU#836068, Vulnerability Notes Database (Last revised Jan. 21, 2009), https://www.kb.cert.org/vuls/id/836068.
[32] Reuters, *supra* note 22.

passwords makes them far harder for hackers to decode.[33] Stronger hashing technology would have made it more difficult for the hackers to get into customer accounts after breaching Yahoo's network, making the attack far less damaging, according to five former employees and outside security experts.[34] But with MD5, there are vast indexes of these pre-computed MD5 hashes—known as "rainbow tables"—freely available online that can be used to quickly crack a large percentage of any MD5 password list.[35] In other words, since the formula for breaking MD5 encryption was known since 2010 or earlier, simple online tools could break even "salted" MD5 codes.

97. So, when Yahoo finally got around to discontinuing MD5 in late summer of 2013, its encryption was already years out-of-date.

98. Yahoo's failure to move away from MD5 in a timely fashion was indicative of systemic problems in Yahoo's security operations. One cybersecurity expert said, "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 altogether braindead idea. It's one of many reasons I've encouraged my friends and family to ditch Yahoo email for years."[36]

99. Indeed, Yahoo's own security personnel often relied on external instant and group messaging programs, like [redacted][37] and [redacted][38] to communicate with each other in order to protect themselves so their communications would not show up on Yahoo's network.

100. As a logical consequence of a highly reckless approach to security, Yahoo's systems suffered a catastrophic breach in 2013, when hackers breached all then-existing

---

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

[34] Stockley, *supra* note 26; Bard, *supra* note 26.

[35] Brian Krebs, My Yahoo Account Was Hacked! Now What?, KrebsonSecurity (Dec. 15, 2016), https://krebsonsecurity.com/2016/12/my-yahoo-account-was-hacked-now-what/.

[36] *Id.*

[37] [redacted]

[38] [redacted]

Yahoo UDB accounts—approximately three billion—stealing the poorly encrypted passwords and other information in the biggest known data breach, by number of records breached, to date. To make matters worse, Yahoo has experienced other security breaches since the 2013 Breach occurred but before either the 2013 Breach or 2014 Breach was made public in 2016. For example, in late December 2013, hackers found an exploit targeting Java in Yahoo's ad network, which affected primarily users in Europe and was infecting roughly 27,000 computers *per hour* at the time of discovery.[39]

101. None of these intrusions or reports prompted Yahoo to comprehensively review and ameliorate its security protocols, allowing the 2014 Breach and the Forged Cookie Breach to occur soon thereafter.

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

102. Yahoo worked with DSW again in 2014, [redacted]

103. These repeated intrusions and warnings from professionals Yahoo itself hired should have driven immediate action. Yahoo took a different tack.

104. [redacted]

[39] Andrew Scurria, European Yahoo Users Victimized in Malware Attack, Law360 (Jan. 6, 2014, 6:02 PM), https://www.law360.com/articles/498914/.

[redacted]

105. [redacted]

106. Then, in late 2014, hackers again accessed Yahoo UDB, accessing and taking information from at least 500 million user accounts. Yahoo knew about the 2014 Breach while it was happening, and even gave it an internal code name: "Siberia":

10.13.14, 11:39	Andrew R.	I need your help!
10.13.14, 12:18	Jeff Z.	whats up bud
10.13.14, 12:18	Andrew R.	I need a good investigation name for this thing
	[...]	
10.13.14, 12:19	Andrew R.	my first thought was codename dingleberry
10.13.14, 12:20	Andrew R.	seems like no matter what shit it's put through it's just hanging on
10.13.14, 12:20	Jeff Z.	haha, clever but no go
10.13.14, 12:20	Andrew R.	hahah | that should be more like our team name
10.13.14, 12:20	Jeff Z.	that's fair
10.13.14, 12:21	Jeff Z.	lets go with a Russian theme, either a city name or famous figure
10.13.14, 12:21	Jeff Z.	since it's the Russians
10.13.14, 12:21	Andrew R.	true
10.13.14, 12:22	Andrew R.	stalin!
10.13.14, 12:23	Jeff Z.	I don't like Stalin

10.13.14, 12:23	Andrew R.	exactly!
10.13.14, 12:25	Andrew R.	just joking.. I'll give it some thought
10.13.14, 12:27	Jeff Z.	I was thinking Project Lenin, Project Runway, or Project Siberia
10.13.14, 12:27	Jeff Z.	the second one is a joke
10.13.14, 12:32	Andrew R.	lol, siberia sounds pretty cool
10.13.14, 12:33	Jeff Z.	lets do it

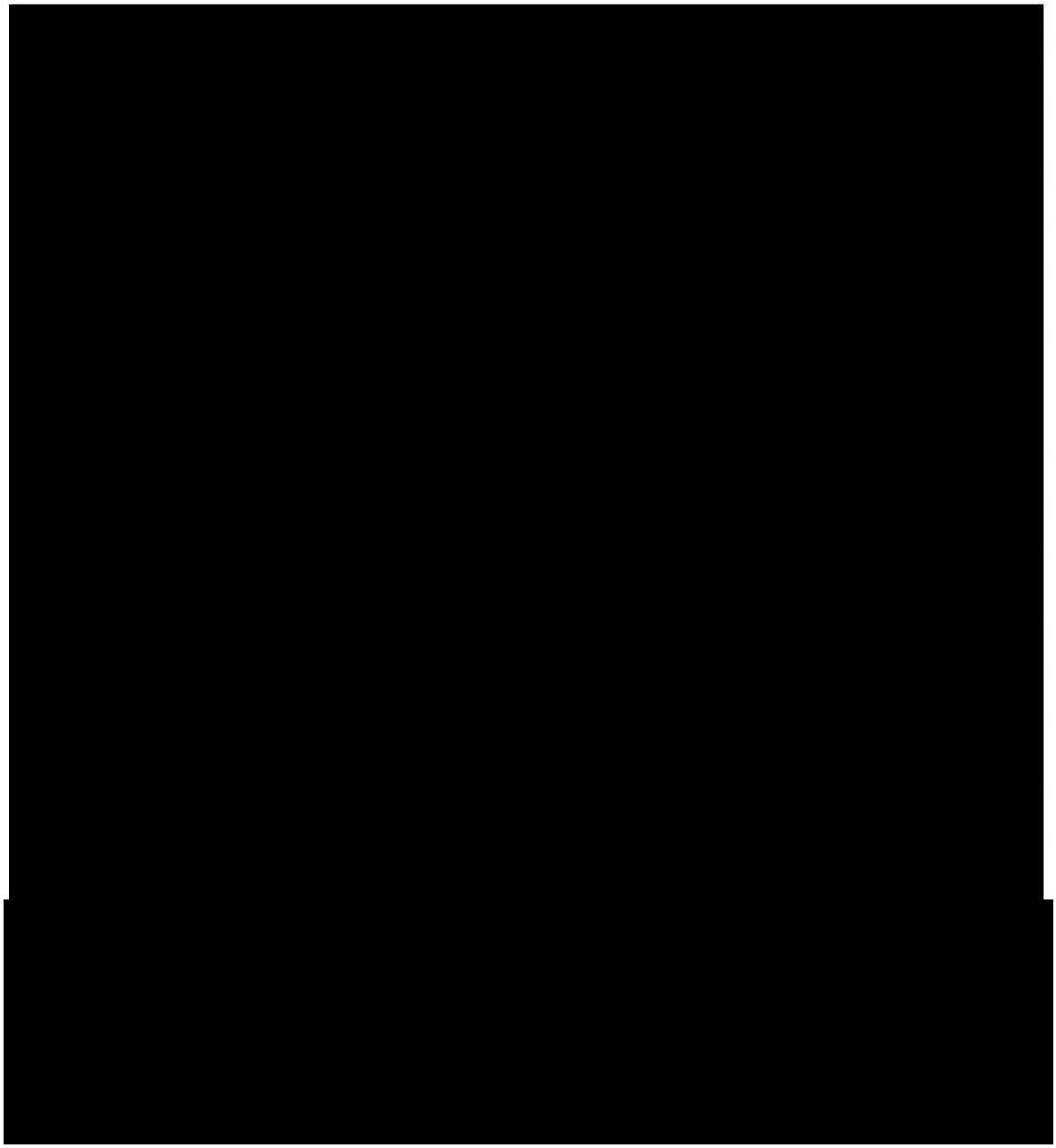
107. Yahoo knew in 2014 that the Siberia intruder(s) had been in its systems for months:

(From internal Yahoo PowerPoint revised Dec. 10, 2014)

108. Not only was Yahoo's CISO aware of the 2014 Breach as it was happening, Yahoo's legal department was also contemporaneously aware of the 2014 Breach. Ron Bell, then *General Counsel for Yahoo*, prepared a document indicating "600m accounts exposed" and "100m transferred off."

109. Yahoo also knew the attackers had actual access to multiple email accounts, including CEO Marissa Mayer's, via the AMT.

110. On December 8, 2014, Yahoo retained DSW yet again. The subsequent report, issued February 10, 2015, showed several waves of attacks, distinguishing between the initial "Siberia" intrusion and a later "Riviera" intrusion during early 2015:



While correctly showing that Yahoo had not, in fact, successfully expelled intruders in 2014, this timeline was still not the full story. That would not come to light for several more years.

111. Adding insult to injury, Yahoo made no disclosures to its users about the breach—no email warnings, no public notices, and no communications, other than emails to "several dozen" individual users telling them to change their passwords and that their

account was "recently accessed by an unauthorized third party." The vast majority of users heard nothing for two full years while Yahoo sat on this information and sophisticated identity thieves had free run of Class members' PII and any confidential information that could be acquired by using that PII. Defendants' failure to take action and notify Class members also prevented unknowing Class members from taking action, thus leaving them even more vulnerable for a long period of time.

112. Yahoo did take *some* action in case news of the 2014 Breach got out—by drafting a reactive press release. Rather than proactively notifying its users (potentially as required by law) and demonstrating that it took security of user data seriously, Yahoo chose to cross its fingers and hope no one found out.

113. [redacted].

114. Bob Lord became CISO at Yahoo in October 2015. He was deeply troubled by what security and endemic culture issues faced him at Yahoo:

- "The decision to keep users at risk over engineering preference is an example of the real culture of security." – Bob Lord, CISO, 1.4.16
- "we don't have a **culture of security** in engineering, or at the executive level" – Bob Lord, CISO, 2.5.16

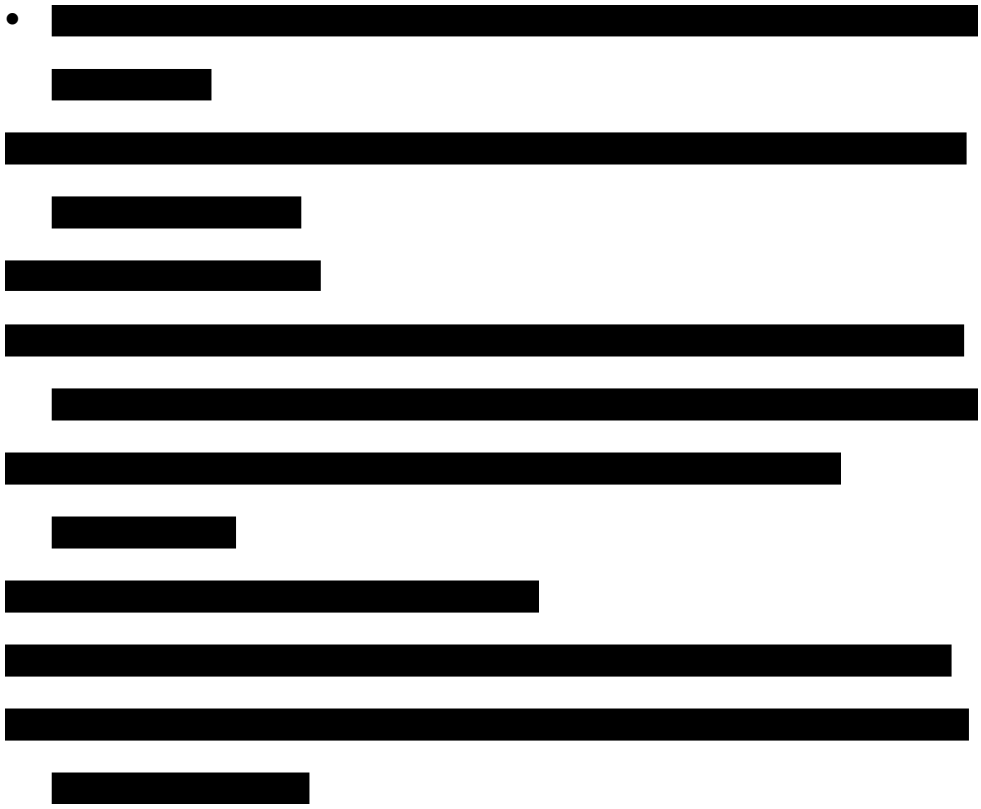
115. Indeed, a brief online chat between Lord and Chris Rohlf neatly sums up the multilayered problems at Yahoo:

From: "lord@yahoo-inc.com" <lord@yahoo-inc.com>
To: <chrisrohlf@yahoo-inc.com>
Subject:
https://docs.google.com/document/d/1LUL2y7dpqnVMAYWKLUwS8SulOkB2JnYQIflZB6rCviY/edit#heading=h.r03mluvyoo46
Received: 26 Jan 2016 15:22:23 +0000 (UTC)

chrisrohlf@yahoo-inc.com(15:02:08 (UTC)):so traditionally ramses, alex, and ricky played siberia very close to the chest bec of the fear of it leaking to nytimes. It was never mine to make the call so I just went along
chrisrohlf@yahoo-inc.com(15:02:13 (UTC)):but i am def behind sharing more with paranoids at a minimum
lord@yahoo-inc.com(15:03:35 (UTC)):This could have been played two ways: (1) tell the org and work with people to improve our posture. (2) Don't tell the org, but have the CEO tell all L2s and L3s "Do what the CISO says. I know it's going to slow things down for a while. Can't say more."
lord@yahoo-inc.com(15:03:45 (UTC)):we did (3) Don't tell anyone, and don't empower the Paranoids
lord@yahoo-inc.com(15:04:07 (UTC)):oh, there's my WTF moment for the day!
chrisrohlf@yahoo-inc.com(15:04:24 (UTC)):yep. i know mm and some L3s knew bec they had to help do stuff like push Duo over a weekend
chrisrohlf@yahoo-inc.com(15:04:31 (UTC)):but yah, we swept it under the carpet
chrisrohlf@yahoo-inc.com(15:04:33 (UTC)):-\
lord@yahoo-inc.com(15:05:45 (UTC)):You can tell Jay's staff "This isn't a theoretical issue. We know for a fact that we're up against nation states, and it can get ugly." If that leaks to the NYTimes, it's a non issue
lord@yahoo-inc.com(15:06:25 (UTC)):I'm sure Son of Siberia is reading this and my mail, but at this point what can you do
chrisrohlf@yahoo-inc.com(15:06:34 (UTC)):agree. and honestly even it did the correct answer imo is "yes of course we have nation state attackers. what do you think we defend against everyday? why do you think we are here?"
chrisrohlf@yahoo-inc.com(15:06:45 (UTC)):hah we actually had an incident we called son of siberia
chrisrohlf@yahoo-inc.com(15:07:23 (UTC)):the technical details of which are so unbelievably lame you would cringe
lord@yahoo-inc.com(15:07:59 (UTC)):where is the final Siberia write up? I can't find a complete document.
lord@yahoo-inc.com(15:08:15 (UTC)):I can find tons of working docs, but not a postortem doc
chrisrohlf@yahoo-inc.com(15:08:30 (UTC)):it is a collection of documents created by rickys team. there may have been one single doc alex took to the board with ramses but if it exists i dont have access
lord@yahoo-inc.com(15:09:24 (UTC)):There was one board deck with a slide called "Nation State Update" in one, but it only had some speaker notes.
lord@yahoo-inc.com(15:09:30 (UTC)):Looks like nothing was shared in writing
chrisrohlf@yahoo-inc.com(15:10:33 (UTC)):the culture here has tended to treat incidents like individual machine compromises and not larger campaigns

116. To be clear, it appears from this exchange that Yahoo's senior executive in charge of information security at Yahoo assumed a nation state actor was contemporaneously reading his Yahoo emails, and Yahoo's employees admitted its approach to the Siberia intrusion was to sweep it under the rug.

117. [redacted]



118. [redacted] Lord further discovered that many of the security vulnerabilities he was facing at Yahoo in 2016 were unchanged from the problems

[redacted]

Yahoo knew about in 2011[40]:

119. Later in the year, Lord reflected on Yahoo's poor approach to information security in response to an inquiry from Verizon regarding security infrastructure at various Yahoo properties:

[redacted]

[40] [redacted]

[redacted].

120. As so many glaring vulnerabilities persisted in Yahoo's security, it is not at all surprising that, sometime in 2015–2016, Yahoo's data security was breached yet again. This time, the attack involved "forged cookies," text files that Yahoo places on user computers when they log in so that users do not need to log in each time they start a new session. Authentication cookies contain information about the user's session with Yahoo, and these cookies can contain a great deal of information about the user, such as whether that user has already authenticated to the company's servers.[41]

121. The attackers in this case, thought to be the same parties involved in the 2014 Breach, were able to forge these authentication cookies, which granted them access to targeted accounts without needing to supply the account's password. In addition, a forged cookie allowed the attackers to remain logged into the hacked accounts for weeks or indefinitely.

122. The Forged Cookie Breach appears to be related to the 2014 Breach because the hackers in the 2014 Breach used some of the data obtained in the 2014 Breach to then forge cookies, help others forge cookies, or use the cookies to gain actual access to specific accounts. Yahoo's failure to notify its users of the 2014 Breach in a timely manner, as well as its failure to adequately harden its data security after the 2014 Breach directly allowed hackers to continue to infiltrate Yahoo's databases into 2015 and 2016.

123. Once again, there was no response from, or disclosure by, Yahoo.

124. Meanwhile, without having disclosed any of these breaches, Yahoo solicited offers to buy the company. Reportedly, Yahoo wanted the offers in by April 19, 2016.[42] Yahoos' failure to disclose the breaches while soliciting offers prevented a mass defection of Yahoo users who might otherwise have left Yahoo after finding out about the breaches, thus allowing Yahoo to artificially inflate its asking price.

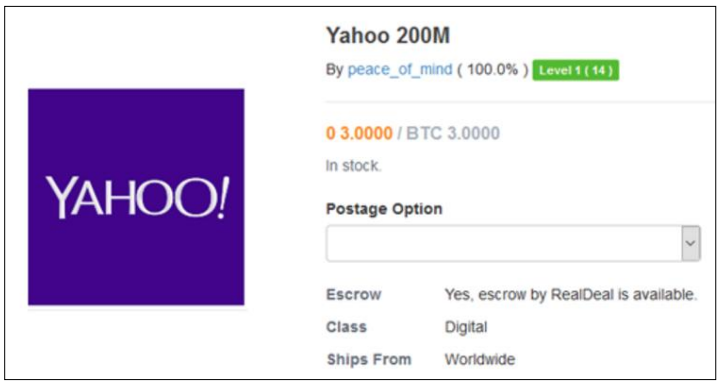
---

[41] Krebs, *supra* note 28.

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

G. ahoo Reveals the 2014 Breach Years After It Happened

125. In August 2016, a hacker identifying himself or herself as "peace_of_mind" posted for sale on the dark web the PII from 200 million Yahoo accounts.



126. The Chief Intelligence Officer of Arizona cybersecurity company InfoArmor, who first spotted the massive database being offered for sale last August, told the *New York Times* in December 2016 that a geographically dispersed hacking group based in Eastern Europe managed to sell copies of the database to three buyers for $300,000 apiece months before Yahoo disclosed the 2014 Breach.[43]

127. Yahoo responded to media inquiries about this by noting that it was "'aware' of the hacker's claims, but ha[d] not confirmed nor denied the legitimacy of the data" offered for sale.[44]

128. Yahoo's internal documents contradicted its public statements. In early June of 2016, Bob Lord (CISO) and Ron Bell (GC) communicated about a document titled "Crystal Castle," which described the Siberia timeline (as shown in paragraph 161, *infra*).

---

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

[44] Joseph Cox, Yahoo 'Aware' Hacker Is Advertising 200 Million Supposed Accounts on Dark Web, MOTHERBOARD (Aug. 1, 2016), http://motherboard.vice.com/read/yahoo-supposed-data-breach-200-million-credentials-dark-web.

The document showed Yahoo was expecting a dump of user credentials at least three months before it publicly announced the 2014 Breach:

129. Finally, on September 22, 2016, more than 3 years after the largest breach (the 2013 Breach), Yahoo publicly announced that the 2014 Breach had occurred. Yahoo said in a statement that "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."[45] This announcement came just two months after Yahoo announced Verizon's plan to acquire its operating assets, and just weeks after Yahoo reported to the SEC that it knew of no incidents of unauthorized access of personal data that might adversely affect the potential acquisition.[46]

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

131. Yahoo also claimed it did not uncover the 2014 Breach for two years, a claim met with immediate skepticism. A September 23, 2016 *Financial Times* report stated that "Yahoo CEO Marissa Mayer has known that Yahoo was investigating a serious data breach since July, but withheld the information from investors, regulators and acquirer Verizon until this week…"[47] Only later would Yahoo concede it knew about the 2014 Breach at the time it took place.

---

[45] Yahoo Security Notice September 22, 2016, Yahoo! Help, https://help.yahoo.com/kb/SLN28092.html (last visited Apr 9, 2017).

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

[47] Harriett Taylor, Yahoo CEO Mayer knew about data breach in July: Report, CNBC (Sept. 23, 2016, 3:51 PM), http://www.cnbc.com/2016/09/23/yahoo-ceo-mayer-knew-about-data-

132. In its 2016 10-K filing with the SEC, Yahoo admitted it had "contemporaneous knowledge" of the 2014 Breach, yet failed to "properly investigate[] and analyze[]" the breach, due in part to "failures in communication, management, inquiry and internal reporting" that led to a "lack of proper comprehension and handling" of the 2014 Breach.[48] Curiously, Yahoo did not disclose in its 10-K that both its CISO and General Counsel were two of the Yahoo executives who possessed that "contemporaneous knowledge."

133. Yahoo had reason to keep any breach under wraps. It struggled for years to compete with more successful technology giants and has now completed a sale of its operating assets and businesses to Verizon for $4.48 billion. By intentionally failing to disclose the breach in a timely manner as required by law, Yahoo misled consumers into continuing to sign up for Yahoo services and products, thus providing Yahoo a continuing income stream and a better chance of finalizing a sale of the company to Verizon.

breach-in-july-report.html.

[48] Yahoo!, Inc. Form 10-K, *supra* note 2, at 47.

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

United States Senate
WASHINGTON, DC 20510

September 27, 2016

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

Dear Ms. Mayer:

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

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

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

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

135. On December 14, 2016, Yahoo finally admitted to the 2013 Breach, though it did not disclose the true scope at the time. Yahoo's Chief Information Security Officer posted the following under an announcement titled "Important Security Information for Yahoo Users":

> As we previously disclosed in November, law enforcement provided us with data files that a third party claimed was Yahoo user data. We analyzed this data with the assistance of outside forensic experts and found that it appears to be Yahoo user data. Based on further analysis of this data by the forensic experts, we believe an unauthorized third party, in August 2013, stole data associated with more than one billion user accounts. We have not been able to identify the intrusion associated with this theft.[49]

136. In the 2013 Breach, hackers obtained, among other things, class members' Yahoo login (ID), Country Code, Recovery E-Mail (linked with the profile), Date of Birth (DOB), Hash of Password (MD5), and Cell phone number and ZIP code if they were provided by the user for password recovery.[50] Although Yahoo asserts that the Breaches did not expose credit card data (and there is little reason at this point to give credence to that claim), the Breaches allowed criminals to obtain passwords and login information for Yahoo users' entire accounts and, thus, obtain the actual content of users' emails, calendars, and contacts. Consequently, any sensitive data or documents contained in those emails, calendars, and contacts could be compromised—not just credit card numbers, but bank

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

[50] InfoArmor: Yahoo Data Breach Investigation, InfoArmor (Sept. 28, 2016), https://www.infoarmor.com/infoarmor-yahoo-data-breach-investigation/.

account numbers, Social Security numbers, driver's license numbers, passport information, birth certificates, deeds, mortgages, and contracts, to name just a few examples.

137. Tyler Moffitt, senior threat research analyst at Webroot, said: "All of the data stolen, including emails, passwords and security questions, make a potent package for identify theft. The main email account has links to other online logins and the average user likely has password overlap with multiple accounts."[51]

138. Moffitt takes little comfort from Yahoo's belated efforts to secure user accounts, stating, "These accounts have been compromised for years and the sheer number of them means they have already been a large source of identity theft. No one should have faith in Yahoo at this point."[52]

139. One analyst, Jeff Williams, CTO of Contrast Security, characterized the 2013 Breach as "the Exxon Valdez of security breaches."[53]

140. In addition to catching the attention of the international media and several governments, these revelations caused Verizon, which was poised to buy Yahoo's operating assets and businesses for $4.83 billion, to demand a $925 million discount on the purchase price. Ultimately, the parties agreed on a $350 million price reduction and an adjustment regarding the parties' respective shares of liability and litigation costs.[54]

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

141. Yahoo quietly divulged the Forged Cookie Breach in its 10-Q filing with the SEC filed November 9, 2016.[55] While filed publicly, the two brief references in the 141-

[51] Samuel Gibbs, Security experts: 'No one should have faith in Yahoo at this point', the guardian (Dec. 15, 2016, 7:29 AM), https://www.theguardian.com/technology/2016/dec/15/security-experts-yahoo-hack.
[52] *Id.*
[53] 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.
[54] Michael Liedtke, Verizon asked for $925M discount for Yahoo data breaches, The Star (Mar. 13, 2017), https://www.thestar.com/business/2017/03/13/verizon-asked-for-925m-discount-for-yahoo-data-breaches.html.
[55] Yahoo!, Inc. 2016 Form 10-Q for quarterly period ended Sept. 30, 2016 (Nov. 9, 2016), at

page filing were overshadowed by the ongoing coverage of the 2014, and then 2013, Breaches. Yahoo failed to notify any affected users at that time.

142. In fact, it appears Yahoo's PR strategy for the Forged Cookie Breach was, once again, to wait and see whether anyone would notice the problem:

Message

From: Suzanne Philion [sphilion@yahoo-inc.com]
Sent: 11/4/2016 6:21:42 PM
To: Yahoo-jf [yahoo-jf@joelefrank.com]
CC: Sheila Tran [tsheila@yahoo-inc.com]; Charles Stewart [chstewart@yahoo-inc.com]
Subject: Back to the rodeo

Team -- thanks for the call just now.

Per our convo, here are the docs we've developed in response to Marissa's request last night. You'll find a draft user notification, press release, backyard/tumblr, and additional FAQs to add to our customer service page. You'll also find linked at the top the industry comparison in terms of how other companies have updated information.

We also developed this PR strat doc on the side to list out our dream stats, tactics, etc.

My strong preference:

- we keep this to a user notification & brief update to Bob's Tumblr with an updated date/time stamp
- we do not issue a press release or update the Q&A online
- we then handle reactively with media
- the phrase "cookie minting" does not need to become a thing: let's not use that publicly

Justification is that we left ourselves plenty of wiggle room in our public communications on 9/22, and this is not a meaty enough update to necessitate a distinct press release:

- our 9/22 press release says: "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."
- we indicate "at least 500M user accounts" in our 9/22 press release

143. Yahoo had drafted notifications pertaining to the Forged Cookie Breach as early as December 15, 2016, but delayed in sending them to affected users.

144. Not until February 2017 did Yahoo begin notifying account holders that their email accounts may have been accessed without the need for a password resulting from the use of forged cookies. Yahoo admitted the Forged Cookie Breach was related to the 2014

40, 69, https://investor.yahoo.net/secfiling.cfm?filingID=1193125-16-764376&CIK=1011006.

Breach.[56] Yahoo's notification informed affected users that "a forged cookie may have been used in 2015 or 2016 to access your account."[57]

145. Yahoo claimed that, since discovering the breach, it had "invalidated the forged cookies and hardened [its] systems to secure them against similar attacks."[58] Yet, users affected by the Forged Cookie Breach were not notified until many months after Yahoo discovered it. [59]

146. Again, data security experts were aghast. One expert, Brian Krebs, saw the Forged Cookie Breach as yet more evidence that Yahoo's online services are unusable[60]:

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

J. The Full Extent of the Fallout from the Breaches is Not Yet Known

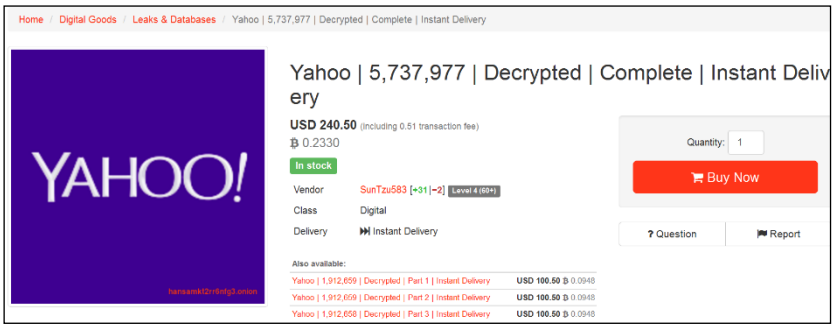
147. Finally, on October 3, 2017, Yahoo/Oath announced that the 2013 Breach had affected every single user account then existing: approximately 3 billion accounts.

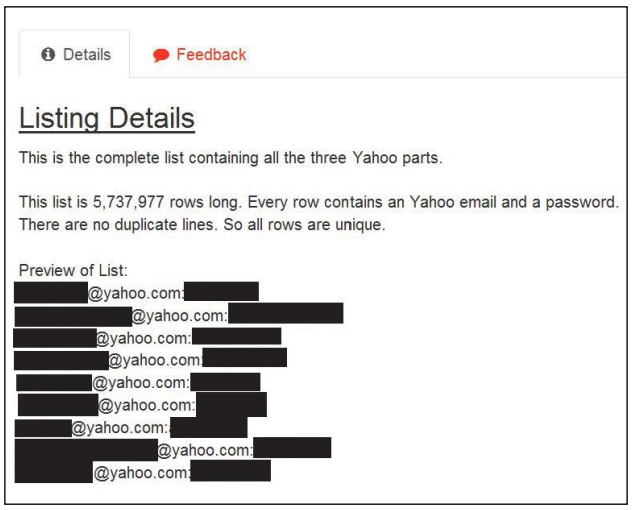
148. Yahoo had first been alerted to the information that would lead to this discovery as early as January 31, 2017 but failed to aggressively pursue it until after the Verizon transaction was completed. Even then, it took months for Yahoo/Oath to determine that closer to three billion, not one billion, accounts had been compromised in 2013.

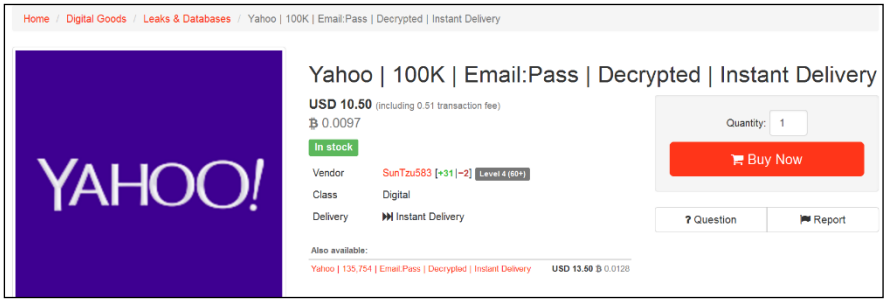
---

[56] Mike Snider & Elizabeth Weise, Yahoo notifies users of 'forged cookie' breach, USA Today (Feb. 15, 2017, 3:59 PM), http://www.usatoday.com/story/tech/news/2017/02/15/yahoo-notifies-users-forged-cookie-breach/97955438/.
[57] *Id.*
[58] Gareth Halfacree, Yahoo warning users of forged cookie account attacks, bit-tech (Feb. 17, 2017), https://www.bit-tech.net/news/bits/2017/02/17/yahoo-warning-forged-cookies/1.
[59] Michelle Castillo, Yahoo's new hack warning comes from a third breach, the company says, CNBC (Feb. 15, 2017, 1:38 PM), http://www.cnbc.com/2017/02/15/yahoo-sends-new-warning-to-customers-about-data-breach.html.
[60] Krebs, *supra* note 28.

149. Unfortunately, for the victims of these Yahoo Data Breaches, their stolen information was still for sale on underground hacker forums as late as summer 2017, [redacted] Their PII will be indefinitely available to those who are willing to pay for it as evidenced by the multiple databases for sale online, as shown below:







150. Making the situation for Class members even worse, Yahoo does not make it easy to delete user email accounts. Although the process may appear straightforward enough, users have to wait at least 90 days after requesting deletion for it to take effect. And even then, the account often remains active. For example, one user tried to delete his Yahoo account, waited 90 days and on the 91st day checked to see if the account was still active.

Unfortunately, and as confirmed by Yahoo, his act of trying to log in to make sure the account was inactive reset the 90-day clock.[61] Other users have also noted that their accounts remained active long after the 90-day period even though they have not logged in.[62]

151. The Data Breaches have had internal effects at Yahoo as well. In Yahoo's 10-K filing with the SEC, Yahoo disclosed that an independent committee of Yahoo's Board of Directors had investigated the Data Breaches and determined that Yahoo's information security team knew, at a minimum, about the 2014 Breach and the Forged Cooke Breach as they were happening, but took no real action in the face of that knowledge.[63]

152. With this admission, Yahoo decided it needed a sacrificial lamb, and that person was Ronald Bell, Yahoo's General Counsel. After the independent committee also determined that the Yahoo legal team "had sufficient information to warrant substantial further inquiry in 2014, and they did not sufficiently pursue it," Bell allegedly "resigned" from his position. Yahoo's 10-K notes that "no payments are being made to Mr. Bell in connection with his resignation."[64] In other words, he received no severance payment.

153. Analysts saw Bell's resignation for what it was—a feeble attempt to create accountability by terminating someone who was not the policy-maker at Yahoo. Yahoo's former head of media, Scott Moore, found the situation "ridiculous."

154. In addition, Yahoo's board of directors, "[i]n response to the Independent Committee's findings related to the 2014" breach, elected not to award CEO Marissa Mayer her 2016 cash bonus, and Mayer has supposedly "offered to forgo any equity award in 2017 given that the 2014 Security Incident occurred during her tenure."[65]

---

[61] Zack Whittaker, Deleting your Yahoo email account? Yeah, good luck with that, ZDNet (Feb. 17, 2017, 10:00 PM), http://www.zdnet.com/article/yahoo-not-deleting-email-accounts-say-users/.
[62] *Id.*
[63] *See* Yahoo!, Inc. Form 10-K, *supra* note 2, at 46-47.
[64] *Id.* at 47.
[65] *Id.*

155. The 2014 Breach and Forged Cookie Breach have since been attributed to two Russian FSB agents, a Russian hacker, and a Canadian hacker. A Justice Department spokesperson said of the breaches, "FSB officers used criminal hackers to gain information that clearly … has intelligence value," and "the criminal hackers used the opportunity to line their own pockets."[66]

156. It appears that the 2014 Breach began with a "spear phishing" email campaign sent to upper-level Yahoo employees.[67] One or more of these employees fell for the bait, and Yahoo's data security was so lax, that this action was enough to hand over the proverbial keys to the kingdom.

157. The hackers then managed to infiltrate Yahoo's UDB, a database containing PII about *all Yahoo users*, including account names, recovery email accounts and phone numbers, password challenge questions and answers, and the account "nonce," a cryptographic value unique to the targeted victim account. The hackers then downloaded the contents of this database on to their own systems. The hackers also gained access to the AMT, a tool that allowed Yahoo to manage all aspects of its users' accounts, including making, logging, and tracking changes in the account, such as password changes.[68]

158. With these tools, the hackers were able to target all kinds of sources, including specific personal targets and general searches such as credit card verification values ("cvv" numbers), and terms such as "credit card," "amex," "visa," "mastercard," "gift card," and

---

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

[67] Indictment, *supra* note 66; *see also* Swati Khandelwal, Yahoo! Hack! How It Took Just One-Click to Execute Biggest Data Breach in History, The Hacker News (Mar. 15, 2017), https://thehackernews.com/2017/03/yahoo-data-breach-hack.html.

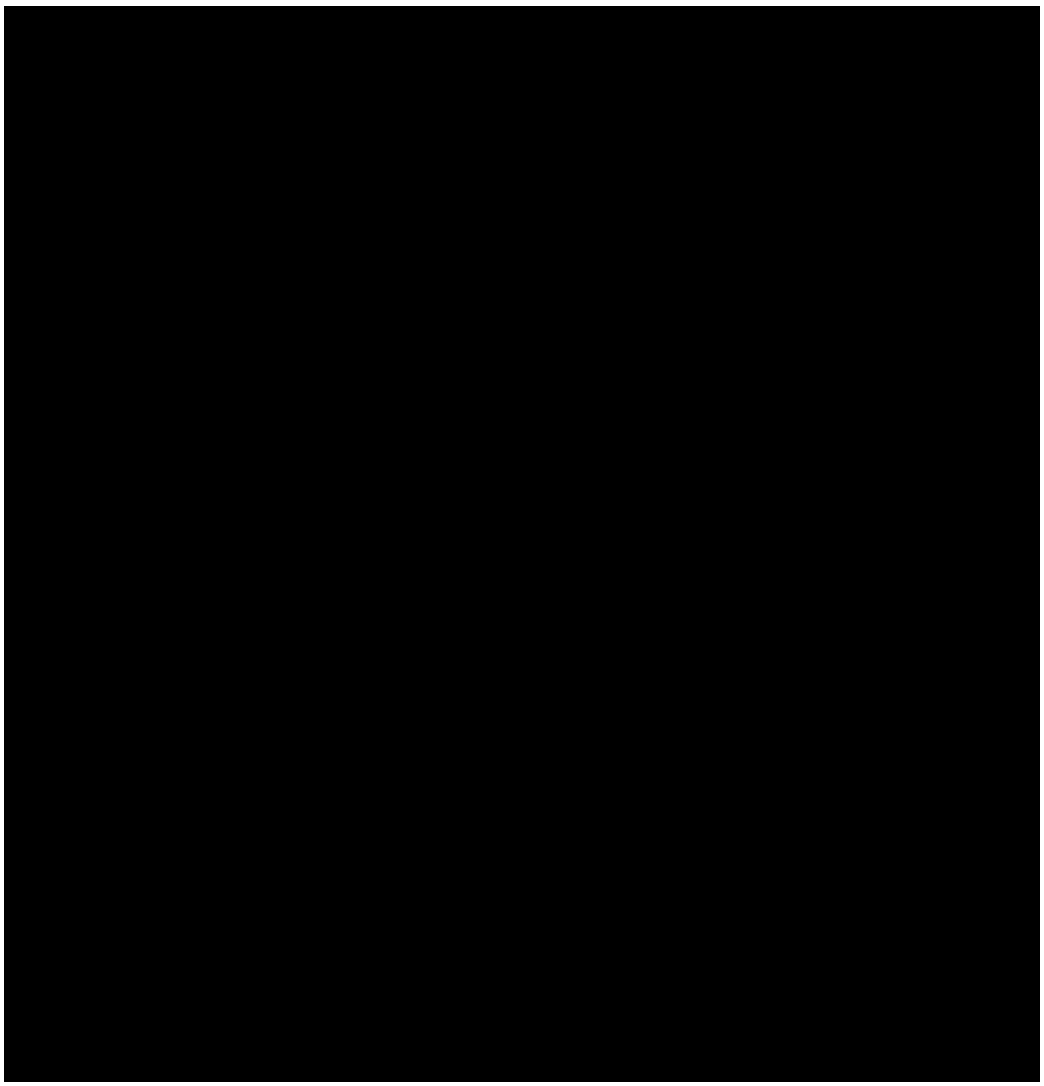
[68] Indictment, *supra* note 66, ¶¶ 22-33; *see also* Martyn Williams, Inside the Russian hack of Yahoo: How they did it, CSO (March 16, 2017, 4:29 AM), http://www.csoonline.com/article/3180762/data-breach/inside-the-russian-hack-of-yahoo-how-they-did-it.html.

others.[69] Through the AMT, they gained direct access to accounts including then-CEO Marissa Mayer's.

159. The hackers also used the Yahoo UDB information to compromise related user accounts with cloud-based services like Apple and webmail providers like Google.[70]

160. Finally, the hackers were able to use the "nonces" to generate forged cookies so that they could gain continuous access to user accounts without having to re-enter password or other security information.[71]

161. In retrospect, it appears the timeline for the Siberia-related intrusions was as follows:



[69] Indictment, *supra* note 66, ¶¶ 22-33.
[70] *Id.*
[71] *Id.*

162. Although Yahoo claims to have plugged the leaks, any fix does not address the fact that Yahoo users' PII is currently in the hands of these hackers, and other miscreants who have obtained Yahoo users' PII by purchase or otherwise. Worse, to date, Yahoo claims it does not—and cannot—determine the root source of the 2013 Breach, in part due to Yahoo's egregious logging procedures.

CLASS ACTION ALLEGATIONS

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

A. The United States Class

> All persons who registered for free Yahoo accounts in the United States and whose PII was accessed, compromised, or stolen from Yahoo in the 2012 Intrusions, the 2013 Breach, the 2014 Breach, or the Forged Cookie Breach.

B. The Small Business Users Class

> All persons who registered for Yahoo Small Business or Aabaco accounts in the United States and whose PII was accessed, compromised, or stolen from Yahoo or Aabaco in the 2012 Intrusions, the 2013 Breach, the 2014 Breach, or the Forged Cookie Breach.

C. The Israel Class

> All persons who registered for Yahoo accounts in the country of Israel and whose PII was accessed, compromised, or stolen from Yahoo in the 2012 Intrusions, the 2013 Breach, the 2014 Breach, or the Forged Cookie Breach.

D. The Paid Users Class

> All persons who registered for paid Yahoo accounts (e.g., "ad-free" accounts or other accounts requiring the user to pay money to Yahoo, but excluding Yahoo or Aabaco Small Business Accounts) in the United States and Israel and whose PII was accessed,

> compromised, or stolen from Yahoo in the 2012 Intrusions, the 2013 Breach, the 2014 Breach, or the Forged Cookie Breach.

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

165. In addition, Plaintiffs Heines and Dugas bring this action on behalf of a **California subclass** defined as:

> All persons in California who registered for Yahoo accounts and whose PII was accessed, compromised, or stolen from Yahoo in the 2012 Intrusions, the 2013 Breach, the 2014 Breach, or the Forged Cookie Breach.

166. Excluded from the Class are Defendants and any entities in which any Defendant or their subsidiaries or affiliates have a controlling interest, and Defendants' officers, agents, and employees. Also excluded from the Class are the judge assigned to this action, and any member of the judge's immediate family.

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

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

i. Whether Defendants represented to the Class that they would safeguard Class members' PII;

ii. Whether Defendants owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII;

iii. Whether Defendants breached a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII;

iv. Whether Class members' PII was accessed, compromised, or stolen in the 2012 Intrusions;

v. Whether Class members' PII was accessed, compromised, or stolen in the 2013 Breach;

vi. Whether Class members' PII was accessed, compromised, or stolen in the 2014 Breach;

vii. Whether Class members' PII was accessed, compromised, or stolen in the Forged Cookie Breach;

viii. Whether Defendants knew about any or all of the Breaches before they were announced to the public and failed to timely notify the public of those Breaches;

ix. Whether Defendants' conduct violated Cal. Civ. Code § 1750, *et seq.*;

x. Whether Defendants' conduct was an unlawful or unfair business practice under Cal. Bus. & Prof. Code § 17200, *et seq.*;

xi. Whether Defendants' conduct violated the Consumer Records Act, Cal. Civ. Code § 1798.80 *et seq.*;

xii. Whether Defendants' conduct violated the Online Privacy Protection Act, Cal. Bus. & Prof. Code § 22575, *et seq.*,

xiii. Whether Defendants' conduct violated § 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, *et seq.*,

xiv. Whether Plaintiffs and the Class are entitled to equitable relief, including, but not limited to, injunctive relief and restitution; and

xv. Whether Plaintiffs and the other Class members are entitled to actual, statutory, or other forms of damages, and other monetary relief.

169. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs individually and on behalf of the members of their respective classes. Similar or identical statutory and common law violations, business

practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous common questions that dominate this action.

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

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

172. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiffs and the other members of their respective classes are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendants, making it impracticable for Class members to individually seek redress for Defendants' wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments, and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

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

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

a. Whether Class members' PII was accessed, compromised, or stolen in the 2012 Intrusions;

b. Whether Class members' PII was accessed, compromised, or stolen in the 2013 Breach;

c. Whether Class members' PII was accessed, compromised, or stolen in the 2014 Breach;

d. Whether Class members' PII was accessed, compromised, or stolen in the Forged Cookie Breach;

e. Whether (and when) Defendants knew about any or all of the Breaches before they were announced to the public and whether Defendants failed to timely notify the public of those Breaches;

f. Whether Defendants' conduct was an unlawful or unfair business practice under Cal. Bus. & Prof. Code § 17200, *et seq.*;

g. Whether Defendants' representations that they would secure and protect the PII and financial information of Plaintiffs and members of the classes were facts that reasonable persons could be expected to rely upon when deciding whether to use Defendants' services;

h. Whether Defendants misrepresented the safety of their many systems and services, specifically the security thereof, and their ability to safely store Plaintiffs' and Class members' PII;

i. Whether Defendants concealed crucial information about their inadequate data security measures from Plaintiffs and the Class;

j. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

k. Whether Plaintiffs and class members in the Paid User Class are consumers within the meaning of Cal. Civ. Code § 1761(d);

l. Whether Defendants' acts, omissions, misrepresentations, and practices were and are likely to deceive consumers;

m. Whether Defendants knew or should have known that they did not employ reasonable measures to keep Plaintiffs' and Class members' PII or financial information secure and prevent the loss or misuse of that information;

n. Whether Defendants failed to "implement and maintain reasonable security procedures and practices" for Plaintiffs' and Class members' PII in violation of California Civil Code section 1798.81.5, subdivision (b) and Section 5 of the FTC Act;

o. Whether Defendants failed to provide timely notice of the 2012 Intrusions, the 2013 Breach, the 2014 Breach, or the Forged Cookie Breach to Plaintiffs and Class members in violation of California Civil Code § 1798.82;

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

q. Whether Defendants owed a duty to Plaintiffs and the Class to safeguard their PII and to implement adequate data security measures;

r. Whether Defendants breached that duty;

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

t. Whether Defendants failed to adhere to their posted privacy policy concerning the care they would take to safeguard Plaintiffs' and Class members' PII in violation of California Business and Professions Code § 22576;

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

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

w. Whether Defendants breached the contract by having inadequate safeguards;

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

y. Whether Defendants breached the implied contract;

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

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

bb. Whether such representations were false with regard to storing and safeguarding Class members' PII; and

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

CHOICE OF LAW

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

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

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

177. In accordance with the choice of law provision, Yahoo has stipulated that California common law and statutory law applies to all claims by members of the United States and Paid User Classes as residents of the United States.

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

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

> CHOICE OF LAW AND FORUM (LOCATION OF LAWSUIT)
>
> The Agreement and the relationship between You and the Company shall be **governed by the laws of the State of California without regard to its conflict of law provisions**, and specifically excluding from application to this Agreement that law known as the United Nations Convention on the International Sale of Goods. You and the Company agree to submit to the personal jurisdiction of the courts located within the county of Santa Clara, California.

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

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

> out of or relating to this ATOS or arising out of or relating to the relationship between you and Yahoo regardless of the type of claim.

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

CLAIMS ALLEGED ON BEHALF OF ALL CLASSES

First Claim for Relief

Violation of California's Unfair Competition Law ("UCL") – Unlawful Business Practice

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

182. Plaintiffs[72] repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 181 as though fully stated herein.

183. By reason of the conduct alleged herein, Defendants engaged in unlawful practices within the meaning of the UCL. The conduct alleged herein is a "business practice" within the meaning of the UCL.

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

[72] This count is not brought on behalf of Plaintiffs Rivlin and Granot as their claims were previously dismissed with prejudice. (ECF No. 215 at 16).

185. Defendants stored the PII of Plaintiffs and members of their respective Classes in Defendants' electronic and consumer information databases. Defendants falsely represented to Plaintiffs and members of the Classes that their PII databases were secure and that class members' PII would remain private. Defendants misleadingly represented that they had "physical, electronic, and procedural safeguards that comply with federal regulations to protect personal information about you."[73] Yahoo further misrepresented that it "deploy[ed] industry standard physical, technical, and procedural safeguards that comply with relevant regulations to protect [Class members'] personal information" Defendants knew or should have known they did not employ reasonable, industry standard, and appropriate security measures that complied "with federal regulations" and that would have kept Plaintiffs' and the other Class members' PII and financial information secure and prevented the loss or misuse of Plaintiffs' and the other class members' PII and financial information. Indeed, at the time of the 2012 Intrusions and the 2013 Breach, Yahoo's data encryption protocol, known as MD5, was widely discredited and had been proven, many years prior, easy to break. Additionally, Yahoo's corporate culture discouraged expenditures that would make their data protection and encryption measures effective.

186. Even without these misrepresentations, Plaintiffs and Class members were entitled to assume, and did assume Defendants would take appropriate measures to keep their PII safe. Defendants did not disclose at any time that Plaintiffs' PII was vulnerable to hackers because Defendants' data security measures were inadequate and outdated, and Defendants were the only ones in possession of that material information, which they had a duty to disclose. Defendants violated the UCL by misrepresenting, both by affirmative conduct and by omission, the safety of its many systems and services, specifically the security thereof, and their ability to safely store Plaintiffs' and Class members' PII. Defendants also violated the UCL by failing to implement reasonable and appropriate security measures or follow industry standards for data security, failing to comply with its own posted privacy policies,

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

and by failing to immediately notify Plaintiffs and the other Class members of the 2014 and Forged Cookie Data Breaches. If Defendants had complied with these legal requirements, Plaintiffs and the other Class members would not have suffered the damages related to the 2012 Intrusions, the 2013 Breach, the 2014 Breach, the Forged Cookie Breach, and consequently from, Defendants' failure to timely notify Plaintiffs and the Class of the 2014 Breach and Forged Cookie Breach.

187. Defendants' acts, omissions, and misrepresentations as alleged herein were unlawful and in violation of, *inter alia*, Cal. Civ. Code § 1798.81.5(b), Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a), Cal. Bus. & Prof. Code § 22576 (as a result of Yahoo failing to comply with its own posted privacy policies), and, as to the Paid Users Class, the Consumer Legal Remedies Act, Cal. Civ. Code § 1750 *et seq*.

188. Plaintiffs and the Class members suffered injury in fact and lost money or property as the result of Defendants' unlawful business practices.[74] In particular, Plaintiffs and Class members have suffered from forged credit applications and tax returns; improper or fraudulent charges to their credit/debit card accounts; hacked emails; and other similar harm, all as a result of the Data Breaches. In addition, their PII was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value. Plaintiffs and Class members have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures. Further, Plaintiffs Neff and Mortensen, and members of the Small Business Class and the Paid Users Class, have lost the benefit of their bargain and purchased services they otherwise would not have, or paid more for supposedly secure services than they would have, had they known the truth regarding Defendants' inadequate data security.

[74] Plaintiffs recognize that this Court ruled out of pocket expenses and the risk of future harm were not sufficient to confer standing under the UCL, and thus certain named plaintiffs lacked standing. However, Plaintiffs have included all named representatives in the "unlawful" and "unfair" UCL causes of action to preserve this issue for appeal.

189. As a result of Defendants' unlawful business practices, violations of the UCL, Plaintiffs Neff and Mortensen and the members of the Paid Users and Small Business classes are entitled to restitution, disgorgement of wrongfully obtained profits and injunctive relief, and all Plaintiffs and all classes and subclass are entitled to injunctive relief.

Second Claim for Relief

Violation of California's Unfair Competition Law ("UCL") – Unfair Business Practice

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

190. Plaintiffs[75] repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 181 as though fully stated herein.

191. By reason of the conduct alleged herein, Defendants engaged in unfair "business practices" within the meaning of the UCL.

192. Defendants stored the PII of Plaintiffs and members of their respective Classes in their electronic and consumer information databases. Defendants represented to Plaintiffs and members of the classes that their PII databases were secure and that class members' PII would remain private. Defendants engaged in unfair acts and business practices by representing that they had "physical, electronic, and procedural safeguards that comply with federal regulations to protect personal information about you."[76] Yahoo further misrepresented that it "deploy[ed] industry standard physical, technical, and procedural safeguards that comply with relevant regulations to protect [Class members'] personal information"

193. Even without these misrepresentations, Plaintiffs and Class members were entitled to, and did, assume Defendants would take appropriate measures to keep their PII safe. Defendants did not disclose at any time that Plaintiffs' PII was vulnerable to hackers because Defendants' data security measures were inadequate and outdated, and Defendants

[75] This count is not brought on behalf of Plaintiffs Rivlin and Granot as their claims were previously dismissed with prejudice. (ECF No. 215 at 16).

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

were the only ones in possession of that material information, which they had a duty to disclose.

194. Defendants knew or should have known they did not employ reasonable measures that would have kept Plaintiffs' and the other Class members' PII and financial information secure and prevented the loss or misuse of Plaintiffs' and the other Class members' PII and financial information. Indeed, at the time of the 2012 Intrusions and the 2013 Breach, Yahoo's data encryption protocol, known as MD5, was widely discredited and had been proven, many years prior, easy to break. Additionally, Defendants' corporate culture discouraged expenditures that would make their data protection and encryption measures effective.

195. Defendants' violated the UCL by misrepresenting, both by affirmative conduct and by omission, the security of their many systems and services, and their ability to safely store Plaintiffs' and Class members' PII. Defendants also violated the UCL by failing to implement and maintain reasonable security procedures and practices appropriate to protect all class members' PII, and by failing to immediately notify Plaintiffs and the other Class members of the Data Breaches. If Defendants followed the industry standards and legal requirements, Plaintiffs and the Class would not have suffered the damages related to the 2012 Intrusions, the 2013 Breach, the 2014 Breach, the Forged Cookie Breach, and consequently from Defendants' failure to timely notify Plaintiffs and the Class of the 2014 Breach and Forged Cookie Breach.

196. Defendants also violated their commitment to maintain the confidentiality and security of the PII of Plaintiffs and their respective Classes, and failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security.

197. **Defendants engaged in unfair business practices under the "balancing test."** The harm caused by Defendants' actions and omissions, as described in detail above, greatly outweigh any perceived utility. Indeed, Defendants' failure to follow basic data security protocols and misrepresentations to consumers about Defendants' data security

cannot be said to have had any utility at all. Thus, for example, there was no utility in Yahoo continuing to use MD5 encryption years after it had been publicly discredited as a viable encryption protocol. Likewise, there was no utility in Yahoo telling the Class that it had "physical, electronic, and procedural safeguards that comply with federal regulations to protect personal information about you," and that it deployed "industry standards," when neither was true. And, there was no utility, other than perhaps to Defendants themselves, in unreasonably waiting to disclose the 2014 Breach and Forged Cookie Breach even though Defendants had contemporaneous knowledge they were happening. All of these actions and omissions were clearly injurious to Plaintiffs and the Class members, directly causing the harms alleged below.

198. **Defendants engaged in unfair business practices under the "tethering test."** Defendants' actions and omissions, as described in detail above, violated fundamental public policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 ("The Legislature declares that ... all individuals have a right of privacy in information pertaining to them.... The increasing use of computers ... has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern.") Defendants' acts and omissions, and the injuries caused by them are thus "comparable to or the same as a violation of the law …" *Cel-Tech Communications, Inc. v. Los Angeles Cellular Telephone Co.* (1999) 20 Cal.4th 163, 187.

199. **Defendants engaged in unfair business practices under the "FTC test."** The harm caused by Defendants' actions and omissions, as described in detail above, is substantial in that it affects hundreds of millions of Class members (not to mention many more hundreds of millions of persons who cannot bring claims in this Court) and has caused those persons to suffer actual harms. Such harms include a substantial risk of identity theft, disclosure of Class members' PII and financial information to third parties without their

consent, diminution in value of their PII, consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures. This harm continues given the fact that Class members' PII remains in Defendants' possession, without adequate protection, and is also in the hands of those who obtained it without their consent. Defendants' actions and omissions violated, *inter alia*, Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45. *See, e.g., F.T.C. v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602, 613 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015); *In re LabMD, Inc.*, FTC Docket No. 9357, FTC File No. 102-3099 (July 28, 2016) (failure to employ reasonable and appropriate measures to secure personal information collected violated § 5(a) of FTC Act); *In re BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148, FTC File No. 042-3160 (Sept. 20, 2005) (same); *In re CardSystems Solutions, Inc.*, FTC Docket No. C-4168, FTC File No. 052-3148 (Sept. 5, 2006) (same); *see also United States v. ChoicePoint, Inc.*, Civil Action No. 1:06-cv-0198-JTC (N.D. Ga. Oct. 14, 2009) ("failure to establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security. confidentiality, and integrity of personal information collected from or about consumers" violates § 5(a) of FTC Act); 15 U.S.C. § 45(n) (defining "unfair acts or practices" as those that "cause[ ] or [are] likely to cause substantial injury to consumers which [are] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.").

200. Plaintiffs and the Class members suffered injury in fact and lost money or property as the result of Defendants' unfair business practices. In particular, Plaintiffs and Class members have suffered from forged credit applications and tax returns; improper or fraudulent charges to their credit/debit card accounts; hacked emails; and other similar harm, all as a result of the Data Breaches. In addition, their PII was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value. Plaintiffs and Class members have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity

theft monitoring, and other expenses relating to identity theft losses or protective measures. Further, Plaintiffs Neff and Mortensen, and members of the Small Business Class and the Paid Users Class, have lost the benefit of their bargain and purchased services they otherwise would not have, or paid more for supposedly secure services than they would have, had they known the truth regarding Defendants' inadequate data security.

201. As a result of Defendants' unfair business practices, violations of the UCL, Plaintiffs Neff and Mortensen and the Paid Users and Small Business classes are entitled to restitution, disgorgement of wrongfully obtained profits and injunctive relief, and all Plaintiffs and all classes and subclass are entitled to injunctive relief.

Third Claim for Relief

Deceit by Concealment — Cal. Civil Code §§ 1709, 1710

202. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 181 as though fully stated herein.

203. As alleged above, Defendants knew their data security measures were grossly inadequate by, at the absolute latest, 2012. At that time, they were warned by both Mandiant and hackers that their systems were extremely vulnerable to attack, facts Defendants already knew given their previous data breaches and security problems. Defendants also learned about the 2014 Breach while it was happening.

204. In response to all of these facts, Defendants chose to do nothing to protect Plaintiffs and the Class or warn them about the security problems and breaches.

205. Defendants had an obligation to disclose to all class members that their Yahoo accounts and PII were an easy target for hackers and Defendants were not implementing measures to protect them. Defendants also had a duty to disclose the 2014 Breach when they knew about it.

206. Defendants did not do these things. Instead, Defendants willfully deceived Plaintiffs and the Class by concealing the true facts concerning their data security, which Defendants were obligated to, and had a duty to, disclose.

207. Had Defendants disclosed the true facts about their dangerously poor data security, Plaintiffs and the Class would have taken measures to protect themselves. Plaintiffs and the Class justifiably relied on Defendants to provide accurate and complete information about Defendants' data security, and Defendants did not.

208. Alternatively, given the gaping security holes in Defendants' services and Defendants' refusal to take measures to even detect those holes, much less fix them, Defendants simply should have shut down their current service. Independent of any representations made by Defendants, Plaintiffs and the Class justifiably relied on Defendants to provide a service with at least minimally adequate security measures and justifiably relied on Defendants to disclose facts undermining that reliance.

209. Rather than cease offering a clearly unsafe and defective service or disclosing to Plaintiffs and the Class that its services were unsafe and users' PII was exposed to theft on a grand scale, Defendants continued on and willfully suppressed any information relating to the inadequacy of their security.

210. These actions are "deceit" under Cal. Civil Code § 1710 in that they are the suppression of a fact, by one who is bound to disclose it, or who gives information of other facts which are likely to mislead for want of communication of that fact.

211. As a result of this deceit by Defendants, they are liable under Cal. Civil Code § 1709 for "any damage which [Plaintiffs and the Class] thereby suffer[]."

212. As a result of this deceit by Defendants, the PII and financial information of Plaintiffs and the Class were compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their PII and financial information was disclosed to third parties without their consent. Plaintiffs and Class members also suffered diminution in value of their PII in that it is now easily available to hackers on the Dark Web. In addition, Plaintiff Neff and the members of the Small Business Users Class and Plaintiff Mortensen and the members of the Paid User Class were damaged to the extent of all or part of the amounts they paid for Defendants' services, because those services were either worth nothing or worth less than was paid for them because of their lack of security. Plaintiffs and the Class

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

213. Defendants' deceit as alleged herein is fraud under Civil Code § 3294(c)(3) in that it was deceit or concealment of a material fact known to the Defendants conducted with the intent on the part of Defendants of depriving Plaintiffs and the Class of "legal rights or otherwise causing injury." As a result, Plaintiffs and the Class are entitled to punitive damages against Defendants under Civil Code § 3294(a).

Fourth Claim for Relief

Negligence

214. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 181 as though fully stated herein.

215. Defendants owed a duty to Plaintiffs and the Class to exercise reasonable care in safeguarding and protecting their PII and keeping it from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties. This duty included, among other things, designing, maintaining, and testing Defendants' security systems to ensure the PII of Plaintiffs' and the Class was adequately secured and protected, including using encryption technologies. Defendants further had a duty to implement processes that would detect a breach of their security system in a timely manner.

216. Defendants knew that the PII of Plaintiffs and the Class was personal and sensitive information that is valuable to identity thieves and other criminals. Defendants also knew of the serious harms that could happen if the PII of Plaintiffs and the Class was wrongfully disclosed, that disclosure was not fixed, or Plaintiffs and the Class were not told about the disclosure in a timely manner.

217. By being entrusted by Plaintiffs and the Class to safeguard their PII, Defendants had a special relationship with Plaintiffs and the Class. Plaintiffs and the Class signed up for Defendants' services and agreed to provide their PII with the understanding that Defendants would take appropriate measures to protect it, and would inform Plaintiffs

and the Class of any breaches or other security concerns that might call for action by Plaintiffs and the Class. But, Defendants did not. Defendants not only knew their data security was inadequate, they also knew they didn't even have the tools to detect and document intrusions or exfiltration of PII. Defendants are morally culpable, given their repeated security breaches, wholly inadequate safeguards, and refusal to notify Plaintiffs and the Class of breaches or security vulnerabilities,

218. Defendants breached their duty to exercise reasonable care in safeguarding and protecting Plaintiffs' and the Class members' PII by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite repeated failures and intrusions, and allowing unauthorized access to Plaintiffs' and the other Class members' PII.

219. Defendants also breached their duty to timely disclose that Plaintiffs' and the other class members' PII had been, or was reasonably believed to have been, stolen or compromised.

220. Defendants' failure to comply with industry and federal regulations further evidences Defendants' negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and the Class members' PII.

221. Defendants' breaches of these duties were not merely isolated incidents or small mishaps. Rather, the breaches of the duties set forth above resulted from a long-term company-wide refusal by Defendants to acknowledge and correct serious and ongoing data security problems. Defendants' corporate culture discouraged its own employees from reporting or fixing security issues and encouraged them to look the other way. Defendants also made a company decision not to disclose the 2014 Breach when they knew about it, but rather to sweep it under the rug as long as possible.

222. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and the Class, their PII would not have been compromised, stolen, and viewed by unauthorized persons. Defendants' negligence was a direct and legal cause of the theft of the PII of Plaintiffs and the Class and all resulting damages.

223. The injury and harm suffered by Plaintiffs and the Class members was the reasonably foreseeable result of Defendants' failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other class members' PII. Defendants knew their systems and technologies for processing and securing the PII of Plaintiffs and the Class had numerous security vulnerabilities.

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

225. Defendants' misconduct as alleged herein is malice or oppression under Civil Code § 3294(c)(1) and (2) in that it was despicable conduct carried on by Defendants with a willful and conscious disregard of the rights or safety of Plaintiffs and the Class and despicable conduct that has subjected Plaintiffs and the Class to cruel and unjust hardship in conscious disregard of their rights. As a result, Plaintiffs and the Class are entitled to punitive damages against Defendants under Civil Code § 3294(a).

Fifth Claim for Relief

Breach of Contract

226. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 181 as though fully stated herein.

227. Yahoo's Privacy Policy is incorporated by reference into its Terms of Service, which forms a binding contract between Yahoo and each user at the time of the creation of an account. The "Security at Yahoo" page is hyperlinked directly from the Yahoo Privacy Policy.

228. Yahoo breached the contract with respect to at least the following four provisions of its Privacy Policy.

- "We are committed to ensuring your information is protected and apply safeguards in accordance with applicable law."
- "Yahoo does not rent, sell, or share personal information about you with other people or non-affiliated companies except to provide products or services you've requested, when we have your permission, or under [certain inapplicable circumstances]."
- "We limit access to personal information about you to employees who we reasonably believe 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."

229. Yahoo further breached the contract with respect to at least the following provisions of the Security at Yahoo page incorporated into the Privacy Policy:

- Promising "a secure user experience . . . ."
- "We deploy industry standard physical, technical, and procedural safeguards that comply with relevant regulations to protect your personal information"

230. Aabaco's Privacy Policy is similarly incorporated by reference into its Terms of Service, forming a binding contract between Aabaco and each user at the time of purchasing any service or product from Aabaco. Aabaco's Terms of Service for 2009 and 2011-2016 are attached to this First Amended Consolidated Class Action Complaint as Exhibits 16-22. Aabaco's Privacy Policy further provides that Aabaco shares PII with Yahoo, and "Yahoo's Privacy Policy governs its use of that information."

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

- "The Company does not rent, sell, or share Personal Information about You with other people or non-affiliated companies except to provide products or services You've requested, when we have Your permission, or under the following circumstances: …"
- "We limit access to Personal Information about You to employees, contractors, or service providers who we believe reasonably need to come into contact with that information to provide products or services to You or in order to do their jobs."
- "We have physical, electronic, and procedural safeguards that comply with federal regulations to protect Personal Information about You."

232. Defendants breached these provisions of the contracts in that they did not have proper safeguards "in accordance with applicable law" to protect Plaintiffs' and Class members' "Personal Information," including, but not limited to, Section 5(a) of the FTC Act, and did not limit access to that information to the specified individuals or entities. Defendants violated their commitment to maintain the confidentiality and security of the PII of Plaintiffs and the class members, and failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security.

233. The 2012, 2013, 2014, and Forged Cookie Data Breaches were a direct and legal cause of the injuries and damages suffered by Plaintiffs and the Class members.

234. Both Yahoo's and Aabaco's Terms of Service purport to impose a limitation of liability on users who agree to the Terms, in which users agree Defendants will not be liable for indirect, punitive, incidental, special, consequential, or exemplary damages. See, Exhs. 1-6, 16-23. These limitations, by their own terms, do not apply to direct damages.

235. Further, to the extent the limitations apply to consequential damages, they are unconscionable under California law.

236. California Commercial Code section 2719(b)(3) provides that a contractual limitation of consequential damages is invalid if it is unconscionable. Unconscionability under California law involves both procedural and substantive unconscionability.

237. Procedural unconscionability under California law focuses on the factors of surprise and oppression. "Oppression" arises from an inequality of bargaining power which results in no real negotiation and 'an absence of meaningful choice.' "Surprise" involves the extent to which the supposedly agreed-upon terms of the bargain are hidden in a prolix printed form drafted by the party seeking to enforce the disputed terms.

238. The Yahoo Terms of Service have both. On the issue of surprise, the liability disclaimers appear on pages 8 and 9 of a 12-page "clickwrap" Terms of Service document—in other words, neither at the front or the back, where users are most likely to see them. The Terms of Service itself is a "clickwrap" agreement where the user must scroll through many pages of contract legalese and then check a box on the computer indicating the user has seen and agreed to the Terms. It is fair to say all Plaintiffs and class members would be surprised to find out Defendants disclaimed even the most basic performance characteristics of their products and services.

239. On the question of oppression, the Terms of Service themselves are contained in an adhesion contract that allows for no form of negotiation or modification. All of Defendants' customers must accept the Terms on a take it or leave it basis.

240. Substantive unconscionability under California law focuses on the one-sidedness or overly harsh effect of the contract term or clause. Again, the disclaimers by Yahoo are inherently one-sided. Among other things Yahoo's disclaimers force its customers to agree that Yahoo's services and software are being provided "as is," and customers are forced to accept that Yahoo disclaims any warranties of any kind. *See, e.g.*, Exh. 3, pp. 7-8. In other words, Yahoo was providing Plaintiffs and the Class with a product or service and then forcing those people to agree the product or service could be completely useless. "Since a product's performance forms the fundamental basis for a sales contract, it is patently unreasonable to assume that a buyer would purchase a standardized mass-produced product

from an industry seller without any enforceable performance standards." *A & M Produce Co. v. FMC Corp.*, 135 Cal. App. 3d 473, 491 (1982).

241. In addition, there is no reasonable commercial justification for such broad disclaimers and limitations on liability. Defendants have obligations under both state and federal law to maintain acceptable levels of data security, so it cannot be commercially reasonable to attempt to evade those legal obligations by way of disclaimers buried in the Terms of Service. Defendants were not selling used products at a yard sale—where an "as is" limitation might be commercially appropriate—they are technology giants providing internet services which they advertised as being safe and sophisticated.

242. Consequential damages are also a clear and well-understood consequence of a data breach, and allowing Yahoo—an internet titan—to compel individual users who just want to sign up for an email address to disclaim them is a commercially unfair re-allocation of risk.

243. Further, the disclaimers are unenforceable under California Civil Code § 1668, which prohibits enforcement of contract terms where the contract attempts to "exempt anyone from responsibility for his own fraud, or willful injury to the person or property of another, or violation of law, whether willful or negligent …"

244. Here, to the extent Defendants are seeking to invoke the disclaimers or limitations on liability to avoid responsibility for their violation of several laws, including Section 5 of the FTC Act, the CRA, and the CLRA, among others, they are "against the policy of the law" and cannot be enforced.

245. Plaintiffs and the other Class members were harmed as the result of Defendants' breach of contract terms outlined above, resulting in the 2012, 2013, 2014, and Forged Cookie Data Breaches, because their PII and financial information were compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their PII and financial information was disclosed to third parties without their consent. Plaintiffs and Class members also suffered diminution in value of their PII in that it is now easily available to hackers on the Dark Web. In addition, Plaintiff Neff and the

members of the Small Business Users Class and Plaintiff Mortensen and the members of the Paid User Class were damaged to the extent of all or part of the amounts they paid for Defendants' services, because those services were either worth nothing or worth less than was paid for them because of their lack of security. Plaintiffs and the Class have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

Sixth Claim for Relief

Breach of Implied Contracts

(In the Alternative to the Claim for Breach of Express Contract)

246. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 181 as though fully stated herein.

247. To the extent that Defendants' Terms of Service and Privacy Policies did not form express contracts, the opening of a Yahoo or Aabaco account created implied contracts between Defendants and the user, the terms of which were set forth by the relevant Terms of Service and Privacy Policy (including the Security at Yahoo page hyperlinked therefrom).

248. Defendants breached such implied contracts by failing to adhere to the terms of the applicable Policy, as described above in Plaintiffs' Fourth Claim for Relief, ¶¶ 226 - 245. Defendants violated their commitment to maintain the confidentiality and security of the PII of Plaintiffs and the Class, and failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security.

249. Plaintiffs and the Class members were harmed as the result of Defendants' breach of the implied contracts because their PII and financial information were compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their PII and financial information was disclosed to third parties without their consent. Plaintiffs and Class members also suffered diminution in value of their PII in that it is now easily available to hackers on the Dark Web. In addition, Plaintiff Neff and the members of the Small Business Users Class and Plaintiff Mortensen and the members of the Paid User Class were damaged to the extent of all or part of the amounts they paid for

Defendants' services, because those services were either worth nothing or worth less than was paid for them because of their lack of security. Plaintiffs and the Class have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures. The Class members are further damaged as their PII remains in Defendants' possession, without adequate protection, and is also in the hands of those who obtained it without their consent.

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

Seventh Claim for Relief

Breach of the Implied Covenant of Good Faith and Fair Dealing

251. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 181 as though fully stated herein.

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

253. Under the express and implied terms of the agreements entered into between Defendants and Plaintiffs and the Class members, Plaintiffs and the Class members were to benefit through the use of Defendants' services, while those Defendants were supposed to benefit through the limited use of users' data for advertising and product enhancement purposes.

254. Defendants exhibited bad faith through their conscious awareness of and deliberate indifference to the risks to Class members' PII, including by (a) using password encryption standards that were long known to be unsafe; (b) taking no serious action in response to past breaches; (c) falling well behind industry standards of cybersecurity; and (d) under-investing in cybersecurity resources despite assurances to its users to the contrary. In doing so, Defendants acted well outside of commercially reasonable norms.

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

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

Eighth Claim for Relief

Declaratory Relief

257. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 181 as though fully stated herein.

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

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

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

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

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

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

259. The grounds for unconscionability of the disclaimers and limitations on liability mentioned above are alleged in paragraphs 234-244, *infra*, and are specifically incorporated herein by reference. The shortened one-year statute of limitations clause is unconscionable and unenforceable for the same reasons and also because it benefits only Defendants and deprives Plaintiffs and the Class of their legal rights. *See, e.g.*, *Circuit City Stores, Inc. v. Adams*, 279 F.3d 889, 894 (9th Cir. 2002) (one-year limitation on employment claims substantively unconscionable).

ADDITIONAL CLAIMS ALLEGED ON BEHALF OF THE SMALL BUSINESS USERS CLASS ONLY

Ninth Claim for Relief

Violation of California's Unfair Competition Law ("UCL") – Fraudulent Business Practice

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

260. Plaintiff Neff repeats, realleges, and incorporates by reference the allegations contained in paragraphs 1 through 181 as though fully stated herein.

261. By reason of the conduct alleged herein, Defendants engaged in fraudulent "business practices" within the meaning of the UCL.

262. Defendants affirmatively represented to Plaintiff Neff and members of the Small Business Users' Class that their PII databases were secure and that Class members' PII would remain private. Defendants engaged in fraudulent acts and business practices by misleadingly representing that they had "physical, electronic, and procedural safeguards that comply with federal regulations to protect personal information about you." Yahoo further misrepresented that it "deploy[ed] industry standard physical, technical, and procedural safeguards that comply with relevant regulations to protect [Class members'] personal information." These representations were false, as detailed in the fact section above.

263. Defendants not only made affirmative misrepresentations but also made fraudulent omissions by concealing the true facts from Plaintiff Neff and members of the Small Business Users' Class. Defendants did not disclose to Plaintiff Neff and members of the Small Business Users' Class that their data security measures were substandard and failed to comply with legal requirements and industry protocols for data security. Defendants also failed to inform Plaintiff Neff and members of the Small Business Users' Class of the 2014 Breach and Forged Cookie Breach in a timely manner despite being required to do so by law. Defendants concealed these material facts from Plaintiff Neff and members of the Small Business Users' Class even though Defendants had exclusive knowledge of them and Plaintiff Neff and members of the Small Business Users' Class could not reasonably have been expected to discover them, and even though they contradicted and rendered untrue Defendants' affirmative representations about data security.

264. Defendants' representations that they would secure and protect the PII of Plaintiff Neff and members of the Small Business Users' Class were facts that reasonable persons could be expected to rely upon when deciding whether to use Defendants' services.

265. Plaintiff Neff and members of the Small Business Users' Class read and relied on these representations in their Terms of Service and the incorporated Privacy Policy in deciding to provide their PII to Defendants. Based on these representations, Plaintiff Neff

and members of the Small Business Users' Class were entitled to, and did, assume Defendants would take appropriate measures to keep their PII safe. Defendants did not disclose at any time that Plaintiffs' PII was vulnerable to hackers because Defendants' data security measures were inadequate and outdated.

266. Specifically, Plaintiff Neff saw, read, and relied on Defendants' representations and warranties regarding the safety and security of his PII in Yahoo's Privacy Policies and Security at Yahoo (for Yahoo small business users), as more fully alleged herein, and would not have signed up for Defendants' services if he had not believed they were secure.

267. Had Plaintiff Neff and members of the Small Business Users' Class known that Defendants' representations about their data security were false, and had Plaintiff Neff and members of the Small Business Users' Class known the material facts Defendants failed to disclose to them about Defendants' substandard data security practices, they would not have provided their PII to Defendants and would not have signed up for Defendants' services.

268. Plaintiff Neff and members of the Small Business Users' Class suffered injury in fact and lost money or property as the result of Defendants' fraudulent business practices. In particular, Plaintiff Neff and members of the Small Business Users' Class have suffered from forged credit applications and tax returns; improper or fraudulent charges to their credit/debit card accounts; hacked emails; and other similar harm, all as a result of the Data Breaches. In addition, their PII was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value. Plaintiff Neff and members of the Small Business Users' Class have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures. Further, Plaintiff Neff and members of the Small Business Users' Class have lost the benefit of their bargain and purchased services they otherwise would not have, or paid

more for supposedly secure services than they would have, had they known the truth regarding Defendants' inadequate data security.

269. As a result of Defendants' fraudulent business practices, violations of the UCL, Plaintiff Neff and members of the Small Business Users' Class are entitled to restitution, disgorgement of wrongfully obtained profits and injunctive relief.

Tenth Claim for Relief

Misrepresentation

270. Plaintiff Neff repeats, realleges, and incorporates by reference the allegations contained in paragraphs 1 through 181 as though fully stated herein.

271. As outlined above, Defendants made numerous representations, in their advertising and in their Privacy Policies, regarding the supposed secure nature of their data security for their small business services. Such representations were false because Defendants utilized outdated encryption, and failed to disclose that they did not use reasonable, industry-standard means, to safeguard against hacking and theft of customer PII.

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

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

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

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

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

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

278. Defendants' misconduct as alleged herein is fraud under Civil Code § 3294(c)(3) in that it was deceit or concealment of a material fact known to the Defendants conducted with the intent on the part of Defendants of depriving Plaintiffs and the Class of "legal rights or otherwise causing injury." In addition, Defendants' misconduct as alleged herein is malice or oppression under Civil Code § 3294(c)(1) and (2) in that it was despicable

conduct carried on by Defendants with a willful and conscious disregard of the rights or safety of Plaintiffs and the Class and despicable conduct that has subjected Plaintiffs and the Class to cruel and unjust hardship in conscious disregard of their rights. As a result, Plaintiffs and the Class are entitled to punitive damages against Defendants under Civil Code § 3294(a).

ADDITIONAL CLAIMS ALLEGED ON BEHALF OF THE PAID USERS CLASS ONLY

Eleventh Claim for Relief

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

(Cal. Civ. Code § 1750, *et seq*.)

279. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 181 as though fully stated herein.

280. The CLRA was enacted to protect consumers against unfair and deceptive business practices. It extends to transactions that are intended to result, or which have resulted, in the sale of goods or services to consumers. Yahoo provided services to Plaintiff Mortensen and members of the Paid Users Class within the meaning of Cal. Civ. Code § 1761(b), and Yahoo's acts, omissions, representations, and practices as described herein fall within the CLRA.

281. Plaintiff Mortensen and the other members of the Paid Users Class are consumers within the meaning of Cal. Civ. Code § 1761(d).

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

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

> (a) The following unfair methods of competition and unfair or deceptive acts or practices undertaken by any person in a transaction intended to result or which results in the sale or lease of goods or services to any consumer are unlawful:
>
> (5) Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have …
>
> (7) Representing that goods or services are of a particular standard, quality, or grade . . . if they are of another.
>
> (14) Representing that a transaction confers or involves rights, remedies, or obligations which it does not have or involve, or which are prohibited by law.
>
> (16) Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

284. Yahoo stored the PII of Plaintiff Mortensen and the other members of the Paid Users Class in its electronic and consumer information databases. Yahoo represented to Plaintiff Mortensen and the other members of the Paid Users Class that its PII databases were secure and that customers' PII would remain private. Yahoo engaged in deceptive acts and business practices by providing in its website that "protecting our systems and our users' information is paramount to ensuring Yahoo users enjoy a secure user experience and maintaining our users' trust." Yahoo represented that it has "physical, electronic, and procedural safeguards that comply with federal regulations to protect personal information about you."[77]

285. Yahoo knew or should have known that it did not employ reasonable measures to keep the PII or financial information of Plaintiff Mortensen and the other members of the Paid Users Class secure and prevent the loss or misuse of that information. In

[77] *See supra* note 73.

fact, Yahoo violated its commitment to maintain the confidentiality and security of the PII of Plaintiff Mortensen and the other members of the Paid Users Class, and failed to comply with its own policies as well as applicable laws, regulations, and industry standards relating to data security.

286. Yahoo's deceptive acts and business practices induced Plaintiff Mortensen and the other members of the Paid Users Class to use Yahoo's online services, and to provide their PII and financial information. But for these deceptive acts and business practices, Plaintiff Mortensen and the other members of the Paid Users Class would not have provided their PII to Yahoo or signed up for the supposedly secure services.

287. Plaintiff Mortensen and the other members of the Paid Users Class were harmed as the result of Yahoo's violations of the CLRA because their PII and financial information were compromised, placing them at a greater risk of identity theft and of their PII and financial information being disclosed to third parties without their consent. Plaintiff Mortensen and the other members of the Paid Users Class also suffered diminution in value of their PII in that it is now easily available to hackers on the Dark Web. Plaintiff Mortensen and the other members of the Paid Users Class have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

288. Plaintiff Mortensen and the other members of the Paid Users Class suffered injury in fact and lost money or property as the result of Yahoo's failure to secure their PII and financial information.

289. As the result of Yahoo's violation of the CLRA, Plaintiff Mortensen and the other members of the Paid Users Class are entitled to compensatory and exemplary damages, an order enjoining Yahoo from continuing the unlawful practices described herein, a declaration that Yahoo's conduct violated the CLRA, attorneys' fees, and the costs of litigation.

290. Pursuant to Civil Code § 1782, on September 30, 2016, in the case of *Myers, et al., v. Yahoo! Inc.*, Case No. 16-cv-2391, filed in the Southern District of California and

consolidated with this action, Plaintiff Paul Dugas, on behalf of himself and all others similarly situated, notified Yahoo in writing by certified mail of the alleged violations of section 1770 and demanded that the same be corrected. In addition, on April 12, 2017, the named Plaintiffs in the original Consolidated Class Action Complaint served an additional notice under section 1782.

ADDITIONAL CLAIMS ALLEGED ON BEHALF OF THE CALIFORNIA SUBCLASS ONLY

Twelfth Claim for Relief

Violation of California's Customer Records Act – Delayed Notification

(Cal. Civ. Code § 1798.82)[78]

291. Plaintiffs Heines and Dugas repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 181 as though fully stated herein.

292. Plaintiffs Heines and Dugas bring this claim on behalf of the California Subclass.

293. Section 1798.82 of the California Civil Code requires any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" to "disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Under section 1798.82, the disclosure "shall be made in the most expedient time possible and without unreasonable delay …"

294. The statute further provides: "Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the

[78] In light of the change in statutory language in 2014 as explained in the Court's August 30, 2017 Order (ECF No. 132 at 63), and Plaintiffs' allegations of concurrent knowledge of the 2012 Intrusions, this count is not alleged in relation to the 2012 Intrusions. Likewise, Plaintiffs acknowledge that this count was dismissed with prejudice as to the 2013 Breach in the Court's March 9, 2018 Order (ECF No. 215 at 41), and accordingly this count is also not alleged as to the 2013 Breach.

data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82(b).

295. Any person or business that is required to issue a security breach notification under the CRA shall meet all of the following requirements:

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

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

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

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

(C) If the information is possible to determine at the time the notice is provided, then any of the following:

(i) the date of the breach,

(ii) the estimated date of the breach, or

(iii) the date range within which the breach occurred. The notification shall also include the date of the notice;

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

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

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

296. The Data Breaches described previously in this First Amended Consolidated Class Action Complaint each constituted a "breach of the security system" of Defendants.

297. As alleged above, Defendants unreasonably delayed informing members of the California subclass about the 2014 Breach, and the Forged Cookies Breach, affecting the confidential and non-public PII and financial information of Plaintiffs Heines and Dugas and the members of the California subclass, after Defendants knew each of those Data Breaches had occurred.

298. Defendants failed to disclose to Plaintiffs Heines and Dugas and the members of the California subclass, without unreasonable delay and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, PII and financial information when Defendants knew or reasonably believed such information had been compromised.

299. Yahoo's ongoing business interests, and in particular its impending sale to Verizon, gave Defendants incentive to conceal the 2014, and Forged Cookie Data Breaches from the public to ensure continued revenue and a high stock price for the sale.

300. Upon information and belief, no law enforcement agency instructed Defendants that notification to Plaintiffs Heines and Dugas and the members of the California subclass would impede its investigation.

301. As a result of Defendants' violation of Cal. Civ. Code § 1798.82, Plaintiffs Heines and Dugas and the members of the California subclass were deprived of prompt notice of the 2014, and Forged Cookie Breaches and were thus prevented from taking appropriate protective measures, such as changing their password, canceling their account, securing identity theft protection, or requesting a credit freeze. These measures would have prevented some or all of the damages suffered by Plaintiffs Heines and Dugas and the members of the California subclass because their stolen information would not have any value to identity thieves.

302. For example, had Defendants provided Plaintiff Heines with prompt notice of the 2014 Breach, rather than two years later, she could have changed her security information and likely could have prevented the theft of her monthly Social Security Disability payment in 2015 and its unauthorized use to buy gift cards.

303. As a result of Defendants' violation of Cal. Civ. Code § 1798.82, Plaintiffs Heines and Dugas and the members of the California subclass suffered incrementally increased damages separate and distinct from those simply caused by the breaches themselves.

304. Plaintiffs Heines and Dugas and the members of the California subclass seek all remedies available under Cal. Civ. Code § 1798.84, including, but not limited to: (a) damages suffered by Plaintiffs and the other class members as alleged above and equitable relief.

PRAYER FOR RELIEF

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

(a) Certifying the United States Class and California Subclass, Small Business Users' Class, Israel Class, and Paid Users Class, and appointing Plaintiffs as Class Representatives;

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

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

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

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

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

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

(h) Awarding Plaintiffs and the Class members punitive damages for the Third, Fourth, Tenth, and Eleventh claims for relief;

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

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

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

JURY TRIAL DEMANDED

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

Dated: July 11, 2019

MORGAN & MORGAN COMPLEX LITIGATION GROUP

/s/ John A. Yanchunis
JOHN A. YANCHUNIS

Attorney for Plaintiffs

On behalf of Plaintiffs' Lead Counsel and Executive Committee