

1 David S. Casey, Jr., SBN 060768
 2 *dcasey@cglaw.com*
 3 Gayle M. Blatt, SBN 122048
 4 *gmb@cglaw.com*
 5 Wendy M. Behan, SBN 199214
 6 *wbehan@cglaw.com*
 7 Angela Jae Chun, SBN 248571
 8 *ajc@cglaw.com*
 9 **Casey Gerry Schenk**
Francavilla Blatt & Penfield, LLP
 110 Laurel Street
 San Diego, CA 92101
 Tel: (619) 238-1811; Fax: (619) 544-9232

10 Deval R. Zaveri, SBN 213501
 11 *dev@zaveritabb.com*
 12 James A. Tabb, SBN 208188
 13 *jimmy@zaveritabb.com*
 14 **Zaveri Tabb, APC**
 402 W. Broadway, Ste. 1950
 San Diego, CA 92101
 Tel: (619) 831-6988; Fax: (619) 239-7800

15 Attorneys for Plaintiffs and the class

16
 17 **United States District Court**
 18 **Northern District of California**
 19 **San Jose Division**

20 **Mali Granot, Yaniv Rivlin, Amiram**
 21 **Tapiro, Deontee King-Sackie, Anna**
 22 **Naupa, Hovahannes Avetisyan,**
 23 **Mahesh Khemlani, and Bekim**
Mehmetaj on behalf of themselves and
 all others similarly situated,

24 Plaintiffs,

25 v.

26 **Yahoo! Inc.**, a Delaware corporation,

27 Defendant.
 28

CASE NO.

**Class Action Complaint for Damages
 and Equitable Relief**

Jury Trial Demanded

1 COME NOW Plaintiffs Mali Granot, Yaniv Rivlin, Amiram Tapiro, Decontee
2 King-Sackie, Anna Naupa, Hovahannes Avetisyan, Mahesh Khemlani, and Bekim
3 Mehmetaj (“Plaintiffs”), on behalf of themselves and all others similarly situated, and
4 for causes of action against the Defendant, complain and allege as follows:

5 **NATURE OF THE ACTION**

6 1. This action is brought to seek redress for damages sustained by Plaintiffs
7 and other members of the class as a result of the failure of Defendant Yahoo! Inc.
8 (“Yahoo” or “Defendant”) to securely store and maintain the personal information of
9 Plaintiffs and the class.

10 2. On September 22, 2016, Yahoo announced that account information from
11 roughly 500 million Yahoo user accounts was stolen by online hackers approximately
12 two years prior. The information included names, email addresses, telephone numbers,
13 birth dates, passwords, and security questions (referred to as “Personal Information”
14 or “PI”) of Yahoo account holders. At the time it was announced, it was believed to be
15 the largest data breach in history.

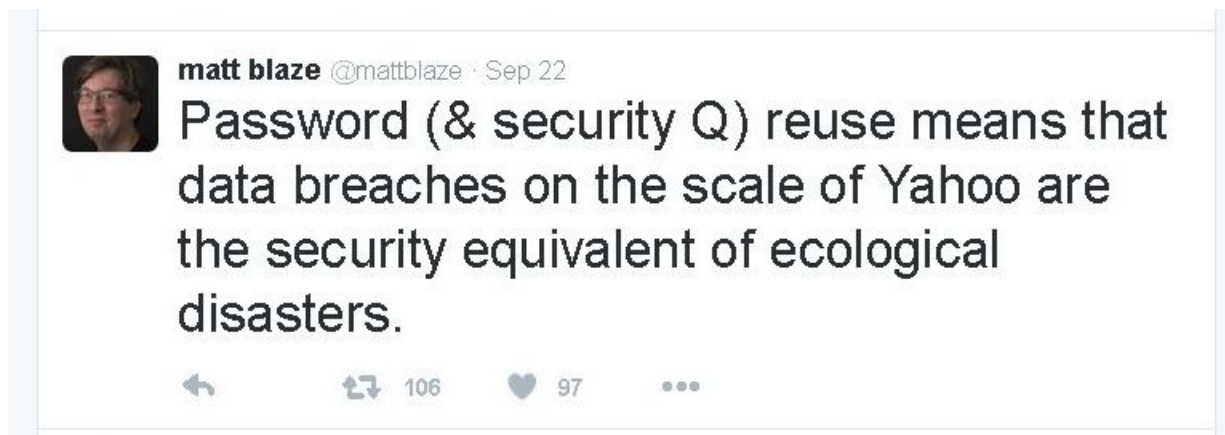
16 3. On December 14, 2016, Yahoo announced that in a separate incident in
17 August 2013, over 1 billion Yahoo users’ account information had been stolen by
18 online hackers. The information included names, email addresses, telephone numbers,
19 birth dates, passwords, and security questions and answers of Yahoo account holders.
20 This is the largest known data breach in history.

21 4. The passwords stolen in August 2013 were encrypted with MD5, a
22 severely compromised encryption algorithm. Yahoo has admitted that, “[a]t the time
23 of the August 2013 incident, we used MD5 to hash passwords. We began upgrading
24 our password protection to bcrypt in the summer of 2013.”

25 5. Security researcher, Brian Krebs said, “[f]or years I have been urging
26 friends and family to migrate off of Yahoo email, mainly because I watched for years
27
28

1 as the company appeared to fall behind its peers in blocking spam and other email-
2 based attacks.”

3 6. Matt Blaze, a cyber security expert and director of the Distributed
4 Systems Lab at the University of Pennsylvania likened the breach announced in
5 September to an “ecological disaster.”



INTRADISTRICT ASSIGNMENT

13
14 7. A substantial part of the events or conduct that give rise to the claims in
15 this action occurred in the county of Santa Clara, and as such this action is properly
16 assigned to the San Jose Division of this Court.

PARTIES

17
18 8. Plaintiff Mali Granot is an individual who resides in Raanana, Israel.
19 Plaintiff was a Yahoo account holder during the time of the data breach. Ms. Granot
20 suffered actual damages as a result of Yahoo’s conduct. Ms. Granot has had her
21 identity compromised and her account set up to receive live chat messages without her
22 authorization, and she has received many such unauthorized messages.

23 9. Plaintiff Yaniv Rivlin is an individual who resides in Tel Aviv, Israel.
24 Mr. Rivlin was a Yahoo account holder during the time of the data breach. He
25 suffered actual damages as a result of Yahoo’s conduct. He paid Yahoo for account
26 forwarding services and hence, shared his financial information with Yahoo.

1 10. Plaintiff Amiram Tapiro is an individual who resides in Tel Aviv, Israel.
2 Mr. Tapiro was a Yahoo and Yahoo Sports account holder during the time of the data
3 breach. He suffered actual damages as a result of Yahoo's conduct.

4 11. Plaintiff Decontee King-Sackie is an individual who resides in Monrovia,
5 Liberia. Ms. King-Sackie was a Yahoo account holder during the time of the data
6 breach. She suffered actual damages as a result of Yahoo's conduct. Her U.S. based
7 debit card information is sent to her email account and since 2013 she had
8 unauthorized bank withdrawals from that account.

9 12. Plaintiff Anna Naupa is an individual who resides in Suva, Fiji. Ms.
10 Naupa was a Yahoo account holder during the time of the data breach. She suffered
11 actual damages as a result of Yahoo's conduct. Ms. Naupa had her bank and credit
12 card information mailed to her Yahoo email account. In 2016, she had several
13 unauthorized charges to her credit card account. Ms. Naupa has also suffered from
14 having embarrassing spam emailed out from her account and has had to handle
15 unauthorized spam.

16 13. Plaintiff Hovhannes Avetisyan is an individual who resides in Yerevan,
17 Armenia. Mr. Avetisyan was a Yahoo account holder during the time of the data
18 breach. He suffered actual damages as a result of Yahoo's conduct. He stores
19 financial information in his account and repeatedly suffered from having to handle
20 unauthorized amounts of spam.

21 14. Plaintiff Mahesh Khemlani is an individual who resides in Panama Oeste,
22 Panama. He suffered actual damages as a result of Yahoo's conduct. Mr. Khemlani
23 was a Yahoo account holder and during the time of the data breach and repeatedly
24 suffered from having to handle unauthorized spam.

25 15. Plaintiff Bekim Mehmetaj is an individual who resides in Prishtina,
26 Kosovo. Mr. Mehmetaj opened his account in Kosovo and was an account holder
27 during the time of the data breach. Mr. Mehmetaj suffered actual damages as a result
28 of Yahoo's conduct.

1 principles. You and Yahoo! Inc. irrevocably consent to the exclusive jurisdiction and
2 venue of the state courts located in Santa Clara County, California, or in the Federal
3 Courts located in the North District of California, USA for all disputes arising out of
4 or relating to this ATOS or arising out of or relating to the relationship between you
5 and Yahoo regardless of the type of claim.”

6 **FACTUAL ALLEGATIONS**

7 22. Yahoo was founded in 1994 as a directory of websites, but developed
8 into a source for searches, email, shopping, and news. Currently, its services attract
9 approximately one billion visitors per month. Yahoo sister sites include, among
10 others, Flickr, Yahoo Finance, and Yahoo Fantasy Sports.

11 23. Yahoo Mail is one of the oldest free email services, and many users have
12 built their digital identities around it, from their bank and stock trading accounts to
13 photo albums and even medical information. Moreover, not only are email addresses
14 used for private communications, but they serve as recovery and log-in credentialing
15 points for accounts on many other websites. Yahoo allows anyone who is over the age
16 of 12 to open a Yahoo account.

17 24. Yahoo is central to many other online services, including ones that
18 require entry of credit card and other financial information, such as the popular Yahoo
19 fantasy sports leagues.

20 25. The Yahoo Fantasy Sports leagues use what Yahoo calls “Yahoo
21 Wallet,” in which users can enter a variety of credit card, debit card, and other account
22 information.

23 26. Plaintiffs and class members signed up for online Yahoo accounts that
24 required them to provide many different sorts of personal information, including, in
25 some cases, debit and credit card information.
26
27
28

1 27. The “Privacy Center” or “Privacy Centre” portion of Yahoo’s website
2 explains the type of personal information it collects directly from its account holders:

3 **Information Collection & Use**

4 **General**

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

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

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

14 <https://policies.yahoo.com/us/en/yahoo/privacy/index.htm>

15 **Information Collection & Use**

16 **General**

17 Yahoo collects personal information when you register with Yahoo, when you use [Yahoo products or services](#),
18 when you visit Yahoo pages or the pages of certain Yahoo partners, and when you enter [promotions or](#)
19 [sweepstakes](#). Yahoo may combine information about you that we have with information we obtain from business
20 partners or other companies.

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

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

27 Yahoo automatically receives and records information from your computer and browser, including your [IP](#)
28 [address](#), Yahoo [cookie](#) information, software and hardware attributes, and the page you request.

 Yahoo uses information for the following general purposes: to customize the advertising and content you see,
 fulfill your requests for products and services, improve our services, contact you, conduct research, and provide
 anonymous reporting for internal and external clients.

Children

 With parental permission, a child under age 13 might have a Yahoo Family Account. Visit [Children's Privacy &](#)
 [Family Accounts](#) to learn more about children's privacy on Yahoo.

<https://policies.yahoo.com/xa/en/yahoo/privacy/index.htm>

1 28. Yahoo also informs its account holders that it does not share personal
2 information:

3 **Information Sharing & Disclosure**

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

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

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

21 <https://policies.yahoo.com/us/en/yahoo/privacy/index.htm>

22 **Information Sharing & Disclosure**

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

- 26 • We provide the information to trusted partners who work on behalf of or with Yahoo under confidentiality
27 agreements. These companies may use your personal information to help Yahoo communicate with you
28 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 ages 18-24 from a particular geographic area.

- Yahoo does not provide any personal information to the advertiser when you interact with or view a targeted
ad. However, by interacting with or viewing an ad you are consenting to the possibility that the advertiser will
make the assumption that you meet the targeting criteria used to display the ad.
- Yahoo advertisers include financial service providers (such as banks, insurance agents, stock brokers and
mortgage lenders) and non-financial companies (such as stores, airlines, and software companies).

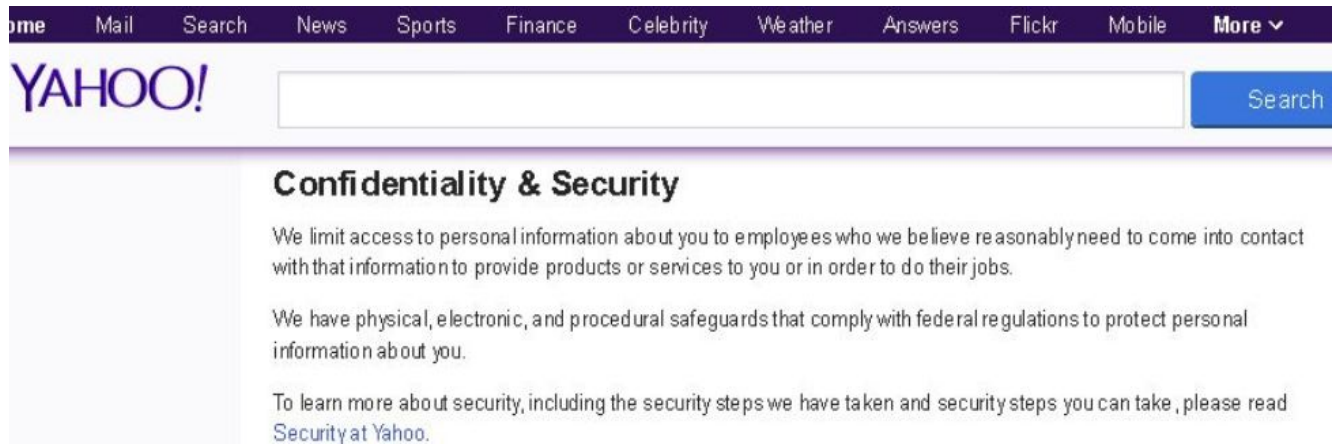
Yahoo works with vendors, partners, advertisers, and other service providers in different industries and
categories of business. For more information regarding providers of products or services that you've requested
please read our detailed [reference links](#).

1 <https://policies.yahoo.com/xa/en/yahoo/privacy/index.htm>

2 29. Yahoo represented to Plaintiffs and the other class members that its PI
3 databases were secure and that customers' PI would remain private. In particular,
4 Yahoo represented that "protecting our systems and our users' information is
5 paramount to ensuring Yahoo users enjoy a secure user experience and maintaining
6 our users' trust."

7 <<https://policies.yahoo.com/us/en/yahoo/privacy/topics/security/index.htm>>.

8 30. Yahoo further assured users that "We have physical, electronic, and
9 procedural safeguards that comply with federal regulations to protect personal
10 information about you."



11
12
13
14
15
16
17
18 <<https://policies.yahoo.com/us/en/yahoo/privacy/index.htm>>

19 **Confidentiality & Security**

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

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

24 To learn more about security, including the security steps we have taken and security steps you can take,
please read [Security at Yahoo.](#)

25 <https://policies.yahoo.com/xa/en/yahoo/privacy/index.htm>

1 31. But, on or about September 22, 2016, Yahoo informed its users that they
2 were victims of a massive data breach, dating back to 2014. Yahoo said in a statement
3 that 500 million user accounts were breached and that “the account information may
4 have included names, email addresses, telephone numbers, dates of birth, hashed
5 passwords (the vast majority with bcrypt) and, in some cases, encrypted or
6 unencrypted security questions and answers.”

7 32. Yahoo also stated that it believed a “state-sponsored actor” was behind
8 the 2014 data breach. However, that was quickly determined not to have been the
9 case.

10 33. On or about December 14, 2016, Yahoo informed its users of a separate
11 breach, that “an unauthorized third party, in August 2013, stole data associated with
12 more than one billion user accounts” and that “this incident is likely distinct from the
13 incident the company disclosed on September 22, 2016.”

14 34. The data stolen in 2013 included names, email addresses, telephone
15 numbers, dates of birth and passwords. According to Yahoo, it only learned of the
16 2013 breach in November 2016, though this information was not shared with its
17 account holders, including Plaintiffs, until on or about December 14, 2016. Around
18 December 20, Plaintiff Rivlin for example, received an email notifying him of the
19 acquisition of his personal information from Yahoo:
20
21
22
23
24
25
26
27
28

YAHOO!

NOTICE OF DATA BREACH

Dear Yaniv,

We are writing to inform you about a data security issue that may involve your Yahoo account information. We have taken steps to secure your account and are working closely with law enforcement.

What Happened?

Law enforcement provided Yahoo in November 2016 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 a broader set of user accounts, including yours. We have not been able to identify the intrusion associated with this theft. We believe this incident is likely distinct from the incident we disclosed on September 22, 2016.

What Information Was Involved?

The stolen user account information may have included names, email addresses, telephone numbers, dates of birth, hashed passwords (using MD5) and, in some cases, encrypted or unencrypted security questions and answers. Not all of these data elements may have been present for your account. The investigation indicates that the stolen information did not include passwords in clear text, payment card data, or bank account information. Payment card data and bank account information are not stored in the system we believe was affected.

What We Are Doing

We are taking action to protect our users:

- We are requiring potentially affected users to change their passwords.
- We invalidated unencrypted security questions and answers so that they cannot be used to access an account.
- We continuously enhance our safeguards and systems that detect and prevent unauthorized access to user accounts.

What You Can Do

We encourage you to follow these security recommendations:

- Change your passwords and security questions and answers for any other accounts on which you used the same or similar information used for your Yahoo account.
- Review all of your accounts for suspicious activity.
- Be cautious of any unsolicited communications that ask for your personal information or refer you to a web page asking for personal information.
- Avoid clicking on links or downloading attachments from suspicious emails.

Additionally, please consider using Yahoo Account Key, a simple authentication tool that eliminates the need to use a password on Yahoo altogether.

For More Information

For more information about this issue and our security resources, please visit the Yahoo Security Issues FAQs page available at https://help.yahoo.com/kb/index?locale=en_CA&page=content&y=PROD_ACCT&id=SLN27925&actp=productlink.

Protecting your information is important to us and we work continuously to strengthen our defenses.

Sincerely,

Bob Lord
Chief Information Security Officer
Yahoo

35. As reported on CNBC, “Due to the scale of the [2014] Yahoo breach, and because users often recycle passwords and security answers across multiple services, cyber security experts warned the impact of the hack could reverberate throughout the internet.” <http://www.cnbc.com/2016/09/23/after-yahoo-data-breach-some-angry-users-close-accounts.html>.

1 36. Neither the 2013 nor the 2014 data breaches were the first threatening
2 Yahoo account holders' personal information. In 2012, Yahoo admitted that more
3 than 450,000 user accounts were compromised. This should have served as a "wake
4 up call" to Yahoo that its protections for users' personal information were inadequate,
5 but Yahoo did not fix the known holes in its security. Instead, Yahoo waited until the
6 summer of 2013 to begin to upgrade its password protection from MD5 to bcrypt.
7 *<https://help.yahoo.com/kb/account/SLN27925.html?impressions=true>.*

8 37. In its September 22, 2016, statement Yahoo claimed it did not uncover
9 that breach until two years after it happened. But Yahoo has been less than
10 forthcoming, as illuminated in a September 23, 2016, Financial Times report that
11 stated that "Yahoo CEO Marissa Mayer has known that Yahoo was investigating a
12 serious data breach since July, but withheld the information from investors, regulators
13 and acquirer Verizon until this week..." *[http://www.cnbc.com/2016/09/23/yahoo-ceo-](http://www.cnbc.com/2016/09/23/yahoo-ceo-mayer-knew-about-data-breach-in-july-report.html)*
14 *[mayer-knew-about-data-breach-in-july-report.html](http://www.cnbc.com/2016/09/23/yahoo-ceo-mayer-knew-about-data-breach-in-july-report.html).*

15 38. Indeed, an article posted on the technology website Motherboard, dated
16 August 1, 2016, stated that "A notorious cybercriminal is advertising 200 million of
17 alleged Yahoo user credentials on the dark web, and the company has said it is
18 'aware' of the hacker's claims, but has not confirmed nor denied the legitimacy of the
19 data." *[http://motherboard.vice.com/read/yahoo-supposed-data-breach-200-million-](http://motherboard.vice.com/read/yahoo-supposed-data-breach-200-million-credentials-dark-web)*
20 *[credentials-dark-web](http://motherboard.vice.com/read/yahoo-supposed-data-breach-200-million-credentials-dark-web).*

21 39. Yahoo had reason to keep any breach under wraps. It struggled for years
22 to compete with more successful technology giants and is now in the midst of a sale of
23 its core business to Verizon for billions of dollars.

24 40. By failing to either discover or disclose the 2013 or 2014 breaches in a
25 timely manner, Yahoo misled consumers into continuing to sign up for Yahoo
26 services and products, thus providing Yahoo a continuing income stream. This, in turn
27 allowed Yahoo to prop up its stock price and maximize profits to Yahoo shareholders
28 (including Yahoo officers) in the sale to Verizon.

1 41. Yahoo’s lack of timeliness caught the attention of several United States
2 senators. On September 27, 2016, following Yahoo’s belated disclosure of the breach,
3 six senators sent Yahoo CEO Marissa Mayer a letter outlining several concerns.

4 42. Senator Mark Warner, a co-founder of Nextel, has further called on the
5 Securities and Exchange Commission to investigate whether Yahoo properly notified
6 the public of the massive breach.

7 43. The type of information compromised in this data breach is highly
8 valuable to perpetrators of identity theft. Names, email addresses, telephone numbers,
9 dates of birth, passwords and security question answers, as well as, obviously, credit
10 and debit card information, can all be used to gain access to a variety of existing
11 accounts and websites. Indeed, named plaintiffs and unnamed class members have
12 suffered a variety of consequences from the breach, including forged credit
13 applications, fake IRS tax returns being filed under the user’s name, fraudulent bank
14 charges, email hacks, and numerous other identity theft-related damages.

15 44. In addition to compromising existing accounts, the class members’ PI can
16 be used by identity thieves to open new financial accounts, incur charges in the name
17 of class members, take out loans, clone credit and debit cards, and other unauthorized
18 activities.

19 45. Identity thieves can also use the PI to harm the class members through
20 embarrassment, blackmail or harassment in person or online, or to commit other types
21 of fraud including obtaining ID cards or driver’s licenses, fraudulently obtaining tax
22 returns and refunds, and obtaining government benefits. A Presidential Report on
23 identity theft from 2008 states that:

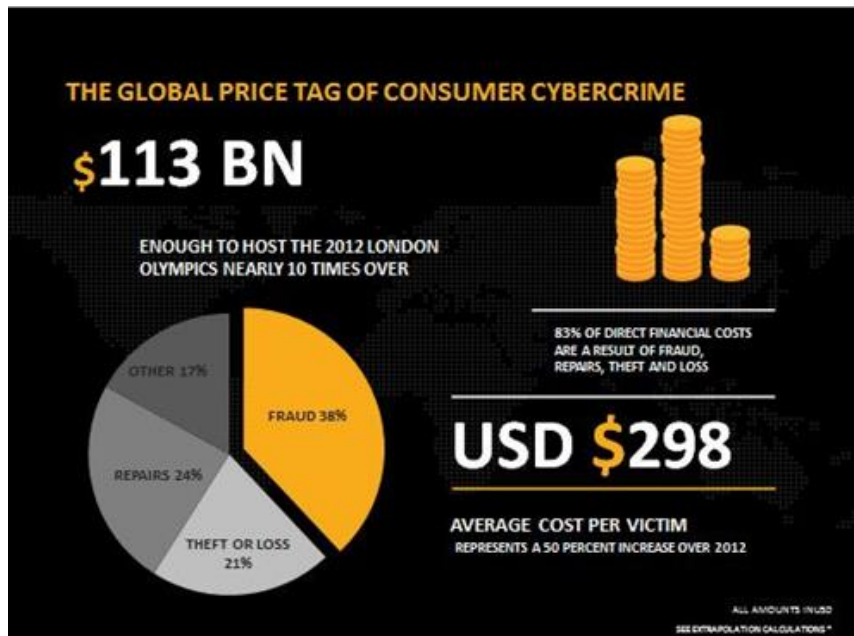
24 In addition to the losses that result when identity thieves fraudulently
25 open accounts or misuse existing accounts, . . . individual victims often
26 suffer indirect financial costs, including the costs incurred in both civil
27 litigation initiated by creditors and in overcoming the many obstacles
28 they face in obtaining or retaining credit. Victims of non-financial

1 identity theft, for example, health-related or criminal record fraud, face
2 other types of harm and frustration.

3 In addition to out-of-pocket expenses that can reach thousands of dollars
4 for the victims of new account identity theft, and the emotional toll
5 identity theft can take, some victims have to spend what can be a
6 considerable amount of time to repair the damage caused by the identity
7 thieves. Victims of new account identity theft, for example, must correct
8 fraudulent information in their credit reports and monitor their reports for
9 future inaccuracies, close existing bank accounts and open new ones, and
10 dispute charges with individual creditors.

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

15 46. To put it into context, the 2013 Norton Report, based on one of the
16 largest consumer
17 cybercrime studies ever
18 conducted, estimated
19 that the global price tag
20 of cybercrime is around
21 \$113 billion, with the
22 average cost per victim
23 being \$298 dollars:



24 47. These
25 problems are
26 exacerbated by the fact
27 that many identity thieves will wait years before attempting to use the personal
28 information they have obtained. A Government Accountability Office (“GAO”) study
found that “stolen data may be held for up to a year or more before being used to

1 commit identity theft.” In order to protect themselves, class members will need to
2 remain vigilant against unauthorized data use for years and decades to come. GAO,
3 Report to Congressional Requesters, at p. 33 (June 2007), available at
4 <www.gao.gov/new.items/d07737.pdf>

5 48. In fact, according to a December 15, 2016, New York Times report,
6 hackers were offering data stolen from Yahoo accounts in the 2013 breach, for sale on
7 the dark web in August 2015. [http://www.nytimes.com/2016/12/15/technology/hacked-](http://www.nytimes.com/2016/12/15/technology/hacked-yahoo-data-for-sale-dark-web.html?_r=0)
8 [yahoo-data-for-sale-dark-web.html?_r=0](http://www.nytimes.com/2016/12/15/technology/hacked-yahoo-data-for-sale-dark-web.html?_r=0)

9 49. Plaintiffs and class members are at risk for identity theft in its myriad
10 forms, *potentially* for the remainder of their lives.

11 50. Yahoo users whose PI has been unlawfully accessed or stolen can—and
12 should—sign up for credit protection services immediately. Such services cost money,
13 however. Yahoo has yet to offer to reimburse such costs for the millions of users
14 affected by the breach.

15 CLASS ACTION ALLEGATIONS

16 51. Plaintiffs bring this lawsuit on behalf of themselves and as a class action
17 on behalf of a proposed Israeli Class, defined as:

18 All Yahoo users in Israel whose personal information was accessed
19 following the data breach that Yahoo announced in a press release on
20 September 22, 2016, and/or the data breach that Yahoo announced in a
21 press release on December 14, 2016.

22 52. Plaintiffs bring this lawsuit on behalf of themselves and as a class action
23 on behalf of a proposed Liberian Class, defined as:

24 All Yahoo users in Liberia whose personal information was accessed
25 following the data breach that Yahoo announced in a press release on
26 September 22, 2016, and/or the data breach that Yahoo announced in a
27 press release on December 14, 2016.

28 53. Plaintiffs bring this lawsuit on behalf of themselves and as a class action
on behalf of a proposed Fijian Class, defined as:

1 All Yahoo users in Fiji whose personal information was accessed
2 following the data breach that Yahoo announced in a press release on
3 September 22, 2016, and/or the data breach that Yahoo announced in a
4 press release on December 14, 2016.

5 54. Plaintiffs bring this lawsuit on behalf of themselves and as a class action
6 on behalf of a proposed Panamanian Class:

7 All Yahoo users in Panama whose personal information was accessed
8 following the data breach that Yahoo announced in a press release on
9 September 22, 2016, and/or the data breach that Yahoo announced in a
10 press release on December 14, 2016.

11 55. Plaintiffs bring this lawsuit on behalf of themselves and as a class action
12 on behalf of a proposed Armenian Class:

13 All Yahoo users in Armenia whose personal information was accessed
14 following the data breach that Yahoo announced in a press release on
15 September 22, 2016, and/or the data breach that Yahoo announced in a
16 press release on December 14, 2016.

17 56. Plaintiffs also bring this lawsuit on behalf of themselves and as a class
18 action on behalf of a proposed Kosovar Class:

19 All Yahoo users in Kosovo whose personal information was accessed
20 following the data breach that Yahoo announced in a press release on
21 September 22, 2016, and/or the data breach that Yahoo announced in
22 a press release on December 14, 2016.

23 57. Collectively, the Israeli, Liberian, Fijian, Panamanian, Armenian, and
24 Kosovar Classes will be referred to as “the Class.”

25 58. Excluded from the Class are Defendants and any entities in which
26 Defendant or their subsidiaries or affiliates have a controlling interest; Defendant’s
27 officers, agents, and employees; attorneys for Plaintiffs and the Class; the judicial
28 officer to whom this action is assigned and any member of the Court’s staff and
emotional distress.

1 59. **Numerosity:** The members of the Class are so numerous that joinder of
2 all members would be impracticable. Plaintiffs reasonably believe that class members
3 number millions of people. As such, class members are so numerous that joinder of all
4 members is impractical. The names and addresses of class members are identifiable
5 through documents maintained by Yahoo.

6 60. **Commonality and Predominance:** This action involves common
7 questions of law or fact, which predominate over any questions affecting individual
8 class members, including:

- 9 61. Whether Defendant engaged in the wrongful conduct alleged herein;
- 10 a. Whether Defendant owed a legal duty to Plaintiffs and the other class
11 members to exercise due care in collecting, storing, and safeguarding
12 their Personal Information;
- 13 b. Whether Defendant negligently or recklessly breached legal duties
14 owed to Plaintiffs and the other class members to exercise due care in
15 collecting, storing, and safeguarding their Personal Information and
16 financial information;
- 17 c. Whether Defendant's conduct violated Cal. Civ. Code § 1750 *et seq.*
- 18 d. Whether Defendant's conduct violated Cal. Bus. & Prof. Code §
19 17200 *et seq.*;
- 20 e. Whether Defendant's conduct violated Cal. Civ. Code § 1798.80 *et*
21 *seq.*;
- 22 f. Whether Defendant violated the Stored Communications Act;
- 23 g. Whether Plaintiffs and the other class members are entitled to actual,
24 statutory, or other forms of damages, and other monetary relief; and
- 25 h. Whether Plaintiffs and the other class members are entitled to
26 equitable relief, including, but not limited to, injunctive relief and
27 restitution.
- 28

1 62. Defendant engaged in a common course of conduct giving rise to the
2 legal rights sought to be enforced by Plaintiffs individually and on behalf of the other
3 class members. Similar or identical statutory and common law violations, business
4 practices, and injuries are involved. Individual questions, if any, pale by comparison,
5 in both quantity and quality, to the numerous questions that dominate this action.

6 63. **Typicality:** Plaintiffs' claims are typical of the claims of the other class
7 members because, among other things, Plaintiffs and the other class members were
8 injured through the substantially uniform misconduct by Yahoo. Plaintiffs are
9 advancing the same claims and legal theories on behalf of themselves and all other
10 class members, and there are no defenses that are unique to Plaintiffs.

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

17 65. **Superiority:** A class action is superior to any other available means for
18 the fair and efficient adjudication of this controversy, and no unusual difficulties are
19 likely to be encountered in the management of this matter as a class action. The
20 damages, harm, or other financial detriment suffered individually by Plaintiffs and the
21 other class members are relatively small compared to the burden and expense that
22 would be required to litigate their claims on an individual basis against Defendant,
23 making it impracticable for class members to individually seek redress for
24 Defendant's wrongful conduct. Even if class members could afford individual
25 litigation, the court system could not. Individualized litigation would create a potential
26 for inconsistent or contradictory judgments, and increase the delay and expense to all
27 parties and the court system. By contrast, the class action device presents far fewer
28

1 you.” (<https://policies.yahoo.com/us/en/yahoo/privacy/topics/security/index.htm>);
2 ([https://policies .yahoo.com/us/en/yahoo/privacy/index.htm](https://policies.yahoo.com/us/en/yahoo/privacy/index.htm)).

3 71. Yahoo knew or should have known that it did not employ reasonable
4 measures that would have kept Plaintiffs’ and the other class members’ PI and
5 financial information secure and prevented the loss or misuse of Plaintiffs’ and the
6 other class members’ PI and financial information.

7 72. Yahoo’s representations that it would secure and protect Plaintiffs’ and
8 the other class members’ PI and financial information in its possession were facts that
9 reasonable persons could be expected to rely upon when deciding whether to use
10 Yahoo’s services.

11 73. Defendant violated the UCL by misrepresenting the safety of their many
12 systems and services, specifically the security thereof, and their ability to safely store
13 Plaintiffs’ and Class Members’ PI. Yahoo also violated the UCL by failing to
14 immediately notify Plaintiffs and the other Class members of the data breach. If
15 Plaintiffs and the other Class members had been notified in an appropriate fashion,
16 they could have taken precautions to safeguard their PI.

17 74. Defendant’s acts, omissions, and misrepresentations as alleged herein
18 were unlawful and in violation of, *inter alia*, Cal. Civ. Code § 1750 *et seq.*, Cal. Civ.
19 Code § 1798.80 *et seq.*, and 18 U.S.C. § 2702, and also Cal. Bus. & Prof. Code §
20 22576 (as a result of Yahoo failing to comply with its own posted privacy policy).

21 75. Plaintiffs and the other Class members suffered injury in fact and lost
22 money or property as the result of Defendant’s failure to secure Plaintiffs’ and the
23 other Class members’ PI contained in Defendant’s servers or databases. In particular,
24 Plaintiffs and class members have suffered from forged credit applications and tax
25 returns; improper or fraudulent charges to their credit/debit card accounts; hacked
26 emails; and other similar harm, all as a result of the data breach.

27 76. As a result of Yahoo’s violations of the UCL, Plaintiffs and the other
28 class members are entitled to restitution and injunctive relief.

1 **Second Claim for Relief**

2 **Violation of California’s Consumer Legal Remedies Act (“CLRA”)**

3 **(Cal. Civ. Code § 1750 *et seq.*)**

4 77. Plaintiffs repeat, reallege, and incorporate by reference the allegations
5 contained in each and every paragraph above, as though fully stated herein.

6 78. The CLRA was enacted to protect consumers against unfair and
7 deceptive business practices. It extends to transactions that are intended to result, or
8 which have resulted, in the sale of goods or services to consumers. Yahoo’s acts,
9 omissions, representations and practices as described herein fall within the CLRA.

10 79. Plaintiffs and the other class members are consumers within the meaning
11 of Cal. Civ. Code §1761(d).

12 80. Yahoo’s acts, omissions, misrepresentations, and practices were and are
13 likely to deceive consumers. By misrepresenting the safety and security of their
14 electronic, health, and customer information databases, Yahoo violated the CLRA.
15 Yahoo had exclusive knowledge of undisclosed material facts, namely, that their
16 consumer databases were defective and/or unsecure, and withheld that knowledge
17 from Plaintiffs and the other class members.

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

21 (a) The following unfair methods of competition and unfair or deceptive
22 acts or practices undertaken by any person in a transaction intended to
23 result or which results in the sale or lease of goods or services to any
24 consumer are unlawful:

25 (5) Representing that goods or services have sponsorship,
26 approval, characteristics, ingredients, uses, benefits, or quantities
which they do not have . . .

27 (7) Representing that goods or services are of a particular
28 standard, quality, or grade . . . if they are of another.

1 (14) Representing that a transaction confers or involves rights,
2 remedies, or obligations which it does not have or involve, or
3 which are prohibited by law.

4 (16) Representing that the subject of a transaction has been
5 supplied in accordance with a previous representation when it has
6 not.

7 82. Defendant stored Plaintiffs' and the other class members' PI in its
8 electronic and consumer information databases. Defendant represented to Plaintiffs
9 and the other class members that their PI databases were secure and that customers' PI
10 would remain private. Yahoo engaged in deceptive acts and business practices by
11 providing in its website that "protecting our systems and our users' information is
12 paramount to ensuring Yahoo users enjoy a secure user experience and maintaining
13 our users' trust" and by representing that it has "physical, electronic, and procedural
14 safeguards that comply with federal regulations to protect personal information about
15 you." (<https://policies.yahoo.com/us/en/yahoo/privacy/topics/security/index.htm>);
16 (<https://policies.yahoo.com/us/en/yahoo/privacy/index.htm>).

17 83. Defendant knew or should have known that it did not employ reasonable
18 measures to keep Plaintiffs' and the other class members' Personal Information or
19 financial information secure and prevented the loss or misuse of that information.

20 84. Defendant's deceptive acts and business practices induced Plaintiffs and
21 the other class members to use Yahoo's online services, and to provide their PI and
22 financial information. But for these deceptive acts and business practices, Plaintiffs
23 and the other class members would not have provided that information to Defendant.

24 85. Plaintiffs and the other class members were harmed as the result of
25 Defendant's violations of the CLRA, because their PI and financial information were
26 compromised, placing them at a greater risk of identity theft and their PI and financial
27 information disclosed to third parties without their consent.
28

1 enforcement, as provided in subdivision (c), or any measures necessary to
2 determine the scope of the breach and restore the reasonable integrity of
the data system.

3 (b) Any person or business that maintains computerized data that
4 includes personal information that the person or business does not own
5 shall notify the owner or licensee of the information of any breach of the
6 security of the data immediately following discovery, if the personal
information was, or is reasonably believed to have been, acquired by an
unauthorized person.

7 (c) The notification required by this section may be delayed if a law
8 enforcement agency determines that the notification will impede a
9 criminal investigation. The notification required by this section shall be
10 made after the law enforcement agency determines that it will not
compromise the investigation.

11 (d) Any person or business that is required to issue a security breach
12 notification pursuant to this section shall meet all of the following
requirements:

13 (1) The security breach notification shall be written in plain
14 language.

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

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

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

20 (C) If the information is possible to determine at the time the
21 notice is provided, then any of the following: (i) the date of
22 the breach, (ii) the estimated date of the breach, or (iii) the
23 date range within which the breach occurred. The
notification shall also include the date of the notice.

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

26 (E) A general description of the breach incident, if that
27 information is possible to determine at the time the notice is
28 provided.

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

5 * * * * *

6 (f) Any person or business that is required to issue a security breach
7 notification pursuant to this section to more than 500 California residents
8 as a result of a single breach of the security system shall electronically
9 submit a single sample copy of that security breach notification,
10 excluding any personally identifiable information, to the Attorney
11 General. A single sample copy of a security breach notification shall not
12 be deemed to be within subdivision (f) of Section 6254 of the
13 Government Code.

14 (g) For purposes of this section, “breach of the security of the system”
15 means unauthorized acquisition of computerized data that compromises
16 the security, confidentiality, or integrity of personal information
17 maintained by the person or business. Good faith acquisition of personal
18 information by an employee or agent of the person or business for the
19 purposes of the person or business is not a breach of the security of the
20 system, provided that the personal information is not used or subject to
21 further unauthorized disclosure.

22 91. The breach described previously in this Complaint constituted a “breach
23 of the security system” of Yahoo.

24 92. As alleged above, Yahoo unreasonably delayed informing anyone about
25 the breach of security of Plaintiffs’ and other class members’ confidential and non-
26 public PI and financial information after Defendant knew the breach had occurred.

27 93. Yahoo failed to disclose to Plaintiffs and other class members, without
28 unreasonable delay, and in the most expedient time possible, the breach of security of
their unencrypted, or not properly and securely encrypted, PI and financial
information when they knew or reasonably believed such information had been
compromised.

94. Yahoo’s ongoing business interests, and in particular its impending sale
to Verizon, gave Yahoo incentive to want to conceal the breach from the public to
ensure continued revenue and a high stock price for the sale.

1 95. Upon information and belief, no law enforcement agency instructed
2 Yahoo that notification to Plaintiffs or other class members would impede its
3 investigation.

4 96. Pursuant to Section 1798.84 of the California Civil Code:

5 (a) Any waiver of a provision of this title is contrary to public
6 policy and is void and unenforceable.

7 (b) Any customer injured by a violation of this title may institute a
8 civil action to recover damages.

9 (c) In addition, for a willful, intentional, or reckless violation of
10 Section 1798.83, a customer may recover a civil penalty not to
11 exceed three thousand dollars (\$3,000) per violation; otherwise, the
12 customer may recover a civil penalty of up to five hundred dollars
(\$500) per violation for a violation of Section 1798.83.

13 * * * * *

14 (e) Any business that violates, proposes to violate, or has violated
this title may be enjoined.

15 97. As a result of Defendant's violation of Cal. Civ. Code § 1798.82,
16 Plaintiffs and the other class members incurred economic damages relating to
17 expenses for credit monitoring, loss of use and value of their debit and/or credit cards,
18 and loss of rewards on their debit and/or credit cards.

19 98. Plaintiffs, on behalf of themselves and the class, seeks all remedies
20 available under Cal. Civ. Code § 1798.84, including, but not limited to: (a) damages
21 suffered by Plaintiffs and the other class members as alleged above; (b) statutory
22 penalties of up to \$3,000 per violation for damages for Defendant's willful,
23 intentional, and/or reckless violations of Cal. Civ. Code § 1798.83 (or, at a minimum,
24 up to \$500 per violation); and (c) equitable relief.

25 99. Plaintiffs and the Class also seeks reasonable attorneys' fees and costs
26 under Cal. Civ. Code §1798.84(g).
27
28

1 **Fourth Claim for Relief**

2 **Negligence**

3 100. Plaintiffs repeat, reallege, and incorporate by reference the allegations
4 contained in each and every paragraph above, as though fully stated herein.

5 101. Yahoo owed a duty to Plaintiffs and the other class members to exercise
6 reasonable care in safeguarding and protecting their PI and financial information that
7 was in its possession from being compromised, lost, stolen, misused, and or/disclosed
8 to unauthorized parties. This duty included, among other things, designing,
9 maintaining, and testing Defendant's security systems to ensure that Plaintiffs' and the
10 other class members' PI and financial information was adequately secured and
11 protected. Defendant further had a duty to implement processes that would detect a
12 breach of their security system in a timely manner.

13 102. Yahoo also had a duty to timely disclose to Plaintiffs and the other class
14 members that their PI and financial information had been or was reasonably believed
15 to have been compromised. Timely disclosure was appropriate so that, among other
16 things, Plaintiffs and the other class members could take appropriate measures to
17 cancel or change usernames, pin numbers, and passwords on compromised accounts,
18 to begin monitoring their accounts for unauthorized access, to contact the credit
19 bureaus to request freezes or place alerts, and take any and all other appropriate
20 precautions.

21 103. Yahoo breached is duty to exercise reasonable care in safeguarding and
22 protecting Plaintiffs' and the other class members' PI and financial information by
23 failing to adopt, implement, and maintain adequate security measures to safeguard that
24 information; allowing unauthorized access to Plaintiffs' and the other class members'
25 PI and financial information stored by Defendant; and failing to recognize in a timely
26 manner the breach.

1 104. Yahoo breached its duty to timely disclose that Plaintiffs’ and the other
2 class members’ PI and financial information had been, or was reasonably believed to
3 have been, stolen or compromised.

4 105. Yahoo’s failure to comply with industry regulations and the delay
5 between the date of intrusion and the date Yahoo informed customers of the data
6 breach further evidence Yahoo’s negligence in failing to exercise reasonable care in
7 safeguarding and protecting Plaintiffs’ and the other class members’ PI and financial
8 information.

9 106. But for Defendant’s wrongful and negligent breach of its duties owed to
10 Plaintiffs and the other class members, their PI and financial information would not
11 have been compromised, stolen, and viewed by unauthorized persons.

12 107. The injury and harm suffered by Plaintiffs and the other class members
13 was the reasonably foreseeable result of Defendant’s failure to exercise reasonable
14 care in safeguarding and protecting Plaintiffs’ and the other class members’ PI and
15 financial information. Defendant knew or should have known that their systems and
16 technologies for processing and securing Plaintiffs’ and the other Class members’ PI
17 and financial information had security vulnerabilities.

18 108. As a result of Defendant’s negligence, Plaintiffs and the other class
19 members incurred economic damages, including expenses for credit monitoring,
20 fraudulent charges on credit card or bank accounts, forged IRS returns, loss of use and
21 value of their debit and/or credit cards, and/or other identity theft-related damages.

Fifth Claim for Relief

Violation of Stored Communications Act, 18 U.S.C. § 2702

22
23
24 109. Plaintiffs repeat, reallege, and incorporate by reference the allegations
25 contained in each and every paragraph above, as though fully stated herein.

26 110. The Federal Stored Communications Act (“SCA”) contains provisions
27 that provide consumers with redress if a company mishandles their electronically
28 stored information. The SCA was designed, in relevant part, “to protect individuals’

1 privacy interests in personal and proprietary information.” S. Rep. No. 99-541, at 3
2 (1986), reprinted in 1986 U.S.C.C.A.N. 3555 at 3557.

3 111. Section 2702(a)(1) of the SCA provides that “a person or entity providing
4 an electronic communication service to the public shall not knowingly divulge to any
5 person or entity the contents of a communication while in electronic storage by that
6 service.” 18 U.S.C. § 2702(a)(1).

7 112. The SCA defines “electronic communication service” as “any service
8 which provides to users thereof the ability to send or receive wire or electronic
9 communications.” *Id.* at § 2510(15).

10 113. Through its equipment, Defendant provides an “electronic
11 communication service to the public” within the meaning of the SCA because it
12 provides consumers at large with mechanisms that enable them to send or receive wire
13 or electronic communications concerning their private financial information to
14 transaction managers, card companies, or banks.

15 114. By failing to take commercially reasonable steps to safeguard sensitive
16 private financial information, even after Defendant was aware that customers’ PI and
17 financial information had been compromised, Defendant knowingly divulged
18 customers’ private financial information that was communicated to financial
19 institutions solely for customers’ payment verification purposes, while in electronic
20 storage in Defendant’s payment system.

21 115. Section 2702(a)(2)(A) of the SCA provides that “a person or entity
22 providing remote computing service to the public shall not knowingly divulge to any
23 person or entity the contents of any communication which is carried or maintained on
24 that service on behalf of, and received by means of electronic transmission from (or
25 created by means of computer processing of communications received by means of
26 electronic transmission from), a subscriber or customer of such service.” 18 U.S.C. §
27 2702(a)(2)(A).

1 116. The SCA defines “remote computing service” as “the provision to the
2 public of computer storage or processing services by means of an electronic
3 communication system.” 18 U.S.C. § 2711(2).

4 117. An “electronic communications systems” is defined by the SCA as “any
5 wire, radio, electromagnetic, photo-optical or photo-electronic facilities for the
6 transmission of wire or electronic communications, and any computer facilities or
7 related electronic equipment for the electronic storage of such communications.” 18
8 U.S.C. § 2510(4).

9 118. Defendant provides remote computing services to the public by virtue of
10 its computer processing services for consumer credit and debit card payments, which
11 are used by customers and carried out by means of an electronic communications
12 system, namely the use of wire, electromagnetic, photo-optical or photo-electric
13 facilities for the transmission of wire or electronic communications received from, and
14 on behalf of, the customer concerning customer private financial information.

15 119. By failing to take commercially reasonable steps to safeguard sensitive
16 private financial information, even after Defendant was aware that customers’ PI and
17 financial information had been compromised, Defendant has knowingly divulged
18 customers’ private financial information that was carried and maintained on
19 Defendant’s remote computing service solely for the customer’s payment verification
20 purposes.

21 120. As a result of Defendant’s conduct described herein and their violations
22 of Section 2702(a)(1) and (2)(A), Plaintiffs and the class members have suffered
23 injuries, including lost money and the costs associated with the need for vigilant credit
24 monitoring to protect against additional identity theft. Plaintiffs, on their own behalf
25 and on behalf of the putative class, seeks an order awarding themselves and the class
26 the maximum statutory damages available under 18 U.S.C. § 2707 in addition to the
27 cost for 3 years of credit monitoring services.

28

1 **PRAYER FOR RELIEF**

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

4 (a) Certifying the Class and the Subclass, appointing Plaintiffs as Class
5 Representatives, and appointing their undersigned counsel as Class Counsel;

6 (b) Finding that Defendant’s conduct was negligent, deceptive, unfair, and
7 unlawful as alleged herein;

8 (c) Enjoining Defendant from engaging in the negligent, deceptive, unfair,
9 and unlawful business practices alleged herein;

10 (d) Awarding Plaintiffs and the other class members actual, compensatory,
11 and consequential damages;

12 (e) Awarding Plaintiffs and the other class members statutory damages and
13 penalties;

14 (f) Awarding Plaintiffs and the other class members restitution and
15 disgorgement;

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

18 (h) Awarding Plaintiffs and the other class members pre-judgment and post-
19 judgment interest;

20 (i) Awarding Plaintiffs and the other class members reasonable attorneys’
21 fees and costs, including expert witness fees; and

22 (i) Granting such other relief as the Court deems just and proper.
23
24
25
26
27
28

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

JURY TRIAL DEMANDED

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

Dated: January 4, 2017

Respectfully submitted,

CASEY GERRY SCHENK FRANCAVILLA
BLATT & PENFIELD, LLP

ZAVERI TABB, APC

/s/ Deval R. Zaveri

Attorneys for Plaintiffs