

1 Clayeo C. Arnold, California SBN 65070
 2 carnold@justice4you.com
 3 Joshua H. Watson, California SBN 238058
 4 jwatson@justice4you.com
 5 **CLAYEO C. ARNOLD, A**
 6 **PROFESSIONAL LAW**
 7 **CORPORATION**
 8 865 Howe Avenue
 9 Sacramento, California 95825
 10 T: 916-777-7777
 11 F: 916-924-1829

12 **MORGAN & MORGAN**
 13 **COMPLEX LITIGATION GROUP**
 14 John A. Yanchunis (Pro Hac Vice Forthcoming)
 15 jyanchunis@ForThePeople.com
 16 Ryan J. McGee (Pro Hac Vice Forthcoming)
 17 rmcgee@ForThePeople.com
 18 Jean S. Martin (Pro Hac Vice Forthcoming)
 19 jeanmartin@ForThePeople.com
 20 201 N. Franklin Street, 7th Floor
 21 Tampa, Florida 33602
 22 Telephone: 813/223-5505
 23 813/223-5402 (fax)

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

26 CARLA ECHAVARRIA, an individual and
 27 California Resident, and DERRICK
 28 WALKER, an individual and Virginia
 Resident,

Plaintiffs,

v.

FACEBOOK, INC.

Defendant

CASE NO.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

- (1) UCL – Unlawful Business Practice
- (2) UCL – Unfair Business Practice
- (3) Deceit by Concealment
- (4) Negligence
- (5) California’s Customer Records Act

TABLE OF CONTENTS

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

I. SUMMARY OF THE CASE.....1

II. JURISDICTION AND VENUE.....2

III. PARTIES2

A. Plaintiffs.....2

B. Defendant.....3

IV. FACTUAL BACKGROUND.....3

A. Facebook Collects and Stores PII for its Own Financial Gain3

B. PII is Very Valuable on the Black Market6

**C. Facebook’s Inadequate Data Security Allows the Massive Breach
of 50 Million User Accounts.....9**

V. CLASS ACTION ALLEGATIONS10

VI. CLAIMS ALLEGED ON BEHALF OF ALL CLASSES.....15

First Claim for Relief.....15

Second Claim for Relief.....17

Third Claim for Relief20

Fourth Claim for Relief22

**VII. ADDITIONAL CLAIMS ALLEGED ON BEHALF OF THE
CALIFORNIA SUBCLASS ONLY.....25**

Fifth Claim for Relief.....25

VIII. PRAYER FOR RELIEF.....27

IX. JURY TRIAL DEMANDED.....28

1 For their Class Action Complaint, Plaintiffs Carla Echavarria and Derick Walker, on
2 behalf of themselves and all others similarly situated, allege the following against Defendant
3 Facebook, Inc. (“Facebook”), based on personal knowledge as to Plaintiffs and Plaintiffs’ own
4 acts and on information and belief as to all other matters based upon, *inter alia*, the
5 investigation conducted by and through Plaintiffs’ undersigned counsel:

6 **SUMMARY OF THE CASE**

7 1. Facebook operates a social networking website that allows people to
8 communicate with their family, friends, and coworkers. Facebook develops technologies that
9 facilitate the sharing of information, photographs, website links, and videos. Facebook
10 purports to allow its users the ability to share and restrict information based on their own
11 specific criteria. By the end of 2017, Facebook had more than 2.2 billion active users.
12

13 2. As part of the sign up process and as a consequence of interacting with the
14 network, Facebook’s users create, maintain, and update profiles containing significant amounts
15 of personal information, including their names, birthdates, hometowns, addresses, locations,
16 interests, relationships, email addresses, photos, and videos, amongst others, referred to herein
17 as “PII.”
18

19 3. This case involves the data breach Facebook announced on September 28, 2018,
20 wherein the PII of 50 million users was exposed due to a flaw in Facebook’s code that allowed
21 hackers and other nefarious users to take over user accounts and siphon off Personal
22 Information for unsavory and illegal purposes.

23 4. This Class Action Complaint is filed on behalf of all persons in the United
24 States, described more fully in the following sections, whose PII was compromised in the data
25 breach.
26
27
28

JURISDICTION AND VENUE

1
2 5. This Court has jurisdiction over this action pursuant to the Class Action
3 Fairness Act (“CAFA”), 28 U.S.C. § 1332(d), because the aggregate amount in controversy
4 exceeds \$5,000,000, exclusive of interests and costs, there are more than 100 class members,
5 and at least one class member is a citizen of a state different from Defendants and is a citizen
6 of a foreign state. The Court also has supplemental jurisdiction over the state law claims
7 pursuant to 28 U.S.C. § 1367.

8
9 6. Venue is proper under 28 U.S.C. § 1391(c) because Defendant is a corporation
10 that does business in and is subject to personal jurisdiction in this District. Venue is also proper
11 because a substantial part of the events or omissions giving rise to the claims in this action
12 occurred in or emanated from this District, including the decisions made by Facebook’s
13 governance and management personnel that led to the breach. Further, Facebook’s terms of
14 service governing users in the United States provides for California venue for all claims arising
15 out of Plaintiffs’ relationship with Facebook.

16
17 **PARTIES**

18 **A. Plaintiffs**

19 7. Plaintiff Carla Echavarria (“Echavarria”) is a resident and citizen of California.
20 Plaintiff Echavarria opened a Facebook account and used it for at least five years, entrusting
21 Facebook with and aggregating PII for this time period. On or about September 28, 2018,
22 Plaintiff Echavarria received a notice from Facebook informing her that her account and PII
23 may have been compromised in the data breach. In addition to the damages detailed herein, the
24 data breach has caused Plaintiff Echavarria to be at substantial risk for further identity theft.

25
26 8. Plaintiff Derrick Walker (“Walker”) is a resident and citizen of Virginia.
27 Plaintiff Walker opened a Facebook account and used it for years, entrusting Facebook with
28

1 and aggregating PII for this time period. On or about September 28, 2018, Plaintiff Walker
2 received a notice from Facebook informing his that her account and PII may have been
3 compromised in the data breach. In addition to the damages detailed herein, the data breach
4 has caused Plaintiff Walker to be at substantial risk for further identity theft.

5 **B. Defendant**

6 9. Defendant Facebook, Inc., is a Delaware corporation with its principal
7 executive offices located at 1601 Willow Road, Menlo Park, California 94025. Facebook’s
8 securities trade on the NASDAQ under the ticker symbol “FB.”
9

10 **FACTUAL BACKGROUND**

11 **A. Facebook Collects and Stores PII for its Own Financial Gain**

12 10. This case involves the continuing and absolute disregard with which Defendant
13 Facebook, has chosen to treat the PII of account holders who utilize Facebook’s social media
14 platform. While this information was supposed to be protected, Facebook, without
15 authorization, exposed that information to third parties through lax and non-existent data safety
16 and security policies and protocols.
17

18 11. Facebook’s Terms of Service state that the Facebook user is the owner of all
19 of their data. Facebook’s representation to Plaintiffs and Class Members that “Protecting
20 people’s information is at the heart of everything we do”¹ was in fact a misrepresentation, and
21 one which Plaintiff and Class Members relied upon.

22 12. Facebook represents to its users that: “you have control over who sees what you
23 share on Facebook.”² Facebook represents to its users that: “We have top-rate security
24
25

26 ¹ Matthew Rosenberg, Nicholas Confessore, and Carole Cadwalladr, *How Trump Consultants Exploited the*
27 *Facebook Data of Millions*, THE NEW YORK TIMES (March 17, 2018)
<https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html> (last visited
28 August 30, 2018).

² Facebook, *Privacy Basics*, <https://www.facebook.com/about/basics> (last visited August 30, 2018).

1 measures in place to help protect you and your data when you use Facebook.”³ Facebook
 2 represents to its users that: “Your activity (ex: posting a status or sending a message) is
 3 encrypted, which means it’s turned into code so people can’t access it without your
 4 permission.”⁴ Facebook represents to its users that: “When it comes to your personal
 5 information, we don’t share it without your permission (unless required by law).”⁵ Facebook
 6 represents to its users that: “Facebook gives people control over what they share, who they
 7 share it with, the content they see and experience, and who can contact them.”⁶

8
 9 13. At all relevant times, Facebook has maintained a Data Use Policy on its website.

10 That Data Use Policy advised Facebook users, in part:

11 Granting us permission to use your information not only allows us to provide
 12 Facebook as it exists today, but it also allows us to provide you with innovative
 13 features and services we develop in the future that use the information we
 14 receive about you in new ways. While you are allowing us to use the
 15 information we receive about you, you always own all of your information.
 16 ***Your trust is important to us, which is why we don't share information we***
 17 ***receive about you with others unless we have:***

- 18 • ***received your permission***
- 19 • ***given you notice***, such as by telling you about it in this policy; or
- 20 • removed your name and any other personally identifying information
 21 from it.

22 (Emphases added).⁷

23 14. Even before his statements (and Facebook’s series of written responses) made
 24 to Congress, Facebook’s Chief Executive Mark Zuckerberg, stated “Every piece of content
 25 that you share on Facebook you own. ... You have complete control over who sees it and how
 26 your share it.”⁸ Facebook users, including Plaintiffs and the Class Members, reasonably relied

27 ³ Facebook, *How You’re Protected*, <https://www.facebook.com/about/basics/stay-safe-and-secure/how-youre-protected> (last visited August 30, 2018).

28 ⁴ *Id.*

⁵ *Id.*

⁶ Facebook, *Safety*, <https://www.facebook.com/safety> (last visited August 30, 2018).

⁷ Facebook, *Data Use Policy*, https://www.facebook.com/full_data_use_policy (last visited August 30, 2018)

⁸ Gabriel Dance, Nicholas Confessore, and Michael LaForgia, *Facebook Gave Device Makers Deep Access to Data on Users and Friends*, THE NEW YORK TIMES (June 3, 2018)

1 on Facebook’s representations for the security of their PII in using Facebook and posting PII
2 on Facebook.

3 15. On June 29, 2018, Facebook provided written responses to seven hundred
4 questions the United States House of Representatives Commerce and Energy Committee
5 submitted to Facebook in April 2018. (“June 2018 Responses”).⁹

6 16. In the June 2018 Responses, Facebook identified the types of data its collects
7 from users:

- 8 • Device attributes: information such as the operating system, hardware and
9 software versions, battery level, signal strength, available storage space,
10 browser type, app and file names and types, and plugins.
- 11 • Device operations: information about operations and behaviors performed
12 on the device, such as whether a window is foregrounded or
13 backgrounded, or mouse movements (which can help distinguish humans
14 from bots).
- 15 • Identifiers: unique identifiers, device IDs, and other identifiers, such as
16 from games, apps or accounts people use, and Family Device IDs (or other
17 identifiers unique to Facebook Company Products associated with the
18 same device or account).
- 19 • Device signals: Bluetooth signals, and information about nearby Wi-Fi
20 access points, beacons, and cell towers.
- 21 • Data from device settings: information users allow us to receive through
22 device settings people turn on, such as access to their GPS location,
23 camera, or photos.
- 24 • Network and connections: information such as the name of users’ mobile
25 operator or ISP, language, time zone, mobile phone number, IP address,
26 connection speed and, in some cases, information about other devices that
27 are nearby or on users’ network, so we can do things like help people
28 stream a video.
- Cookie data: data from cookies stored on a user’s device, including cookie
IDs and settings.¹⁰

17. Despite Facebook’s tumultuous 2018—including the Cambridge Analytica
revelations, reading and collecting the contents of messages on Android Devices, and the
device partnerships Facebook secretly entered into to share PII with other, unauthorized

<https://www.nytimes.com/interactive/2018/06/03/technology/facebook-device-partners-users-friends-data.html> (last visited August 30, 2018).

⁹ Facebook, *Letter to House Commerce and Energy Committee*, June 29, 2018, available at <https://docs.house.gov/meetings/IF/IF00/20180411/108090/HHRG-115-IF00-Wstate-ZuckerbergM-20180411-SD003.pdf> (hereinafter, “*Letter to House*”)

¹⁰ *Letter to House*, at p. 112.

1 entities—Facebook’s lax approach to data security resulted in a data breach affected 50 million
2 users (the “September 2018 Data Breach”).

3 18. On March 19, 2018, *Bloomberg* published an article entitled “FTC Probing
4 Facebook For Use of Personal Data, Source Says,” disclosing that the U.S. Federal Trade
5 Commission (“FTC”) was investigating whether Facebook violated the terms of a 2011 FTC
6 consent decree regarding its handling of user data.¹¹

7 19. Under the 2011 settlement with the FTC, Facebook “agreed to get user consent
8 for certain changes to privacy settings as part of a settlement of federal charges that it deceived
9 consumers and forced them to share more Personal Information than they intended.”¹²

10
11 **B. PII is Very Valuable on the Black Market**

12 20. The types of information compromised in the September 2018 Data Breach are
13 highly valuable to identity thieves. The names, email addresses, recovery email accounts,
14 telephone numbers, birthdates, passwords, security question answers, and other valuable PII
15 can all be used to gain access to a variety of existing accounts and websites.

16
17 21. Identity thieves can also use the PII to harm Plaintiffs and Class members
18 through embarrassment, blackmail, or harassment in person or online, or to commit other types
19 of fraud including obtaining ID cards or driver’s licenses, fraudulently obtaining tax returns
20 and refunds, and obtaining government benefits. A Presidential Report on identity theft from
21 2008 states that:

22
23 In addition to the losses that result when identity thieves fraudulently open
24 accounts or misuse existing accounts, . . . individual victims often suffer
25 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

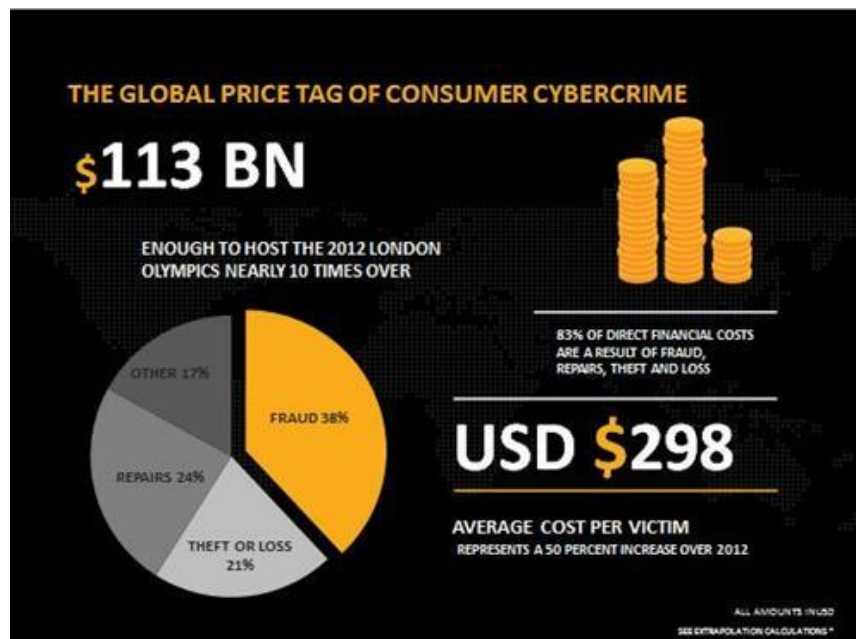
26
27 ¹¹ Bloomberg Markets, *FTC Said to Probe Facebook on Personal Data Use*, Bloomberg (March 19, 2018)
[https://www.bloomberg.com/news/videos/2018-03-20/facebook-said-to-face-ftc-probe-on-use-of-personal-
data-video](https://www.bloomberg.com/news/videos/2018-03-20/facebook-said-to-face-ftc-probe-on-use-of-personal-data-video) (last visited August 30, 2018)

28 ¹² *Id.*

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

2 In addition to out-of-pocket expenses that can reach thousands of dollars for
3 the victims of new account identity theft, and the emotional toll identity
4 theft can take, some victims have to spend what can be a considerable
5 amount of time to repair the damage caused by the identity thieves. Victims
6 of new account identity theft, for example, must correct fraudulent
information in their credit reports and monitor their reports for future
inaccuracies, close existing bank accounts and open new ones, and dispute
charges with individual creditors.¹³

7 22. To put it into context, as demonstrated in the chart below, the 2013 Norton
8 Report, based on one of the
9 largest consumer cybercrime
10 studies ever conducted,
11 estimated that the global price tag
12 of cybercrime was around \$113
13 billion at that time, with the
14 average cost per victim being
15 \$298 dollars. That number will
16 no doubt increase exponentially
17 after the PII of over 50 million users was leaked in the September 2018 Data Breach.
18
19



20 23. The problems associated with identity theft are exacerbated by the fact that
21 many identity thieves will wait years before attempting to use the PII they have obtained.
22 Indeed, in order to protect themselves, Class members will need to remain vigilant against
23 unauthorized data use for years and decades to come.
24
25

26 ¹³ The President's Identity Theft Task Force, Combating Identity Theft: A Strategic Plan,
27 Federal Trade Commission, 11 (April 2007),
28 <http://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf>.

1 24. Once stolen, PII can be used in a number of different ways. One of the most
2 common is that it is offered for sale on the “dark web,” a heavily encrypted part of the Internet
3 that makes it difficult for authorities to detect the location or owners of a website. The dark
4 web is not indexed by normal search engines such as Google and is only accessible using a Tor
5 browser (or similar tool), which aims to conceal users’ identities and online activity. The dark
6 web is notorious for hosting marketplaces selling illegal items such as weapons, drugs, and
7 PII.¹⁴ Websites appear and disappear quickly, making it a very dynamic environment.

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

12 26. In addition to PII, a hacked Facebook account can be very valuable to cyber
13 criminals. Since Facebook accounts are linked to myriad accounts, a hacked Facebook account
14 could open up a number of other accounts to an attacker.
15
16
17
18
19
20
21
22
23
24
25
26

27 ¹⁴ Brian Hamrick, The dark web: A trip into the underbelly of the internet, WLWT News
28 (Feb. 9, 2017 8:51 PM), <http://www.wlwt.com/article/the-dark-web-a-trip-into-the-underbelly-of-the-internet/8698419>.

1 **C. Facebook’s Inadequate Data Security Allows the Massive Breach of 50 Million**
2 **User Accounts**

3 27. On September 28, 2018, Facebook announced the “previously unreported
4 attack on its network,” exposing the PII of “nearly 50 million users.”¹⁵

5 28. Facebook claims it discovered the vulnerability “earlier this week,” that
6 Facebook entirely fixed the vulnerability, and law enforcement was notified.¹⁶

7 29. Facebook, however, did not know the origin of or identify the hackers. In fact,
8 Facebook had not full assessed the scope of the attack, despite its representations that the
9 vulnerability was fixed.¹⁷

10 30. The vulnerability Facebook disclosed was a bug in its site’s “view as” feature,
11 which permits users to view their profiles posing as someone else, which, ironically, was built
12 in to give users more control over their privacy.¹⁸

13 31. In a conference call, Guy Rosen, a vice president of product management at
14 Facebook, admitted the September 2018 Data Breach was “complex,” and “leveraged three
15 separate bugs in Facebook’s code that, once compounded, provided widespread access to user
16 accounts.”¹⁹

17 32. Senator Mark Warner, a Democrat from Virginia, stated “This is another
18 sobering indicator that Congress needs to step up and take action to protect the privacy and
19
20
21
22
23

24 ¹⁵ Chris Mills, Facebook Says New Hack Leded Data of 50 Million Users, BGR (Sept. 28,
25 2018) <https://bgr.com/2018/09/28/facebook-data-breach-2018-yep-another-one/>

26 ¹⁶ Mike Issac and Sheera Frenkel, Facebook Network is Breached, Putting 50 Million Users’
27 Data at Risk, NY Times (Sept. 28, 2018),
<https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html>

28 ¹⁷ Id.

¹⁸ Id.

¹⁹ Id.

1 security of social media users,” underscoring the lack of protections Facebook and other
2 companies have when storing and securing the PII of millions of United States citizens.²⁰

3 33. Unfortunately, despite numerous lapses in their approach to data security,
4 Facebook still lacks the safeguards and protections for users’ PII, and that information remains
5 at risk today and into the future, until Facebook is compelled to secure the PII stored on
6 millions of United States citizens.

7 **CLASS ACTION ALLEGATIONS**

8 34. Pursuant to Rule 23(b)(2), (b)(3) and (c)(4) of the Federal Rules of Civil
9 Procedure, Plaintiffs, individually and on behalf of all others similarly situated, bring this
10 lawsuit on behalf of themselves and as a class action on behalf of the following classes:
11

12 **A. The United States Class**

13 All persons who registered for Facebook accounts in the United
14 States and whose PII was accessed, compromised, or stolen from
15 Facebook in the September 2018 Data Breach.

16 35. In addition, Plaintiffs Echavarria brings this action on behalf of a **California**
17 **subclass** defined as:

18 All persons in California who registered for Facebook accounts and
19 whose PII was accessed, compromised, or stolen from Facebook in
20 the September 2018 Data Breach.

21 36. Excluded from the Class are Defendant and any entities in which any Defendant
22 or its subsidiaries or affiliates have a controlling interest, and Defendant’s officers, agents, and
23 employees. Also excluded from the Class are the judge assigned to this action, members of the
24 judge’s staff, and any member of the judge’s immediate family.

25 37. **Numerosity:** The members of each Class are so numerous that joinder of all
26 members of any Class would be impracticable. Plaintiffs reasonably believe that Class
27

28 ²⁰ Id.

1 members number hundreds of millions of people or more in the aggregate and well over 1,000
2 in the smallest of the classes. The names and addresses of Class members are identifiable
3 through documents maintained by Defendants.

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

- 7
- 8 i. Whether Defendant represented to the Class that it would safeguard Class
9 members' PII;
 - 10 ii. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise
11 due care in collecting, storing, and safeguarding their PII;
 - 12 iii. Whether Defendant breached a legal duty to Plaintiffs and the Class to
13 exercise due care in collecting, storing, and safeguarding their PII;
 - 14 iv. Whether Class members' PII was accessed, compromised, or stolen in the
15 September 2018 Data Breach;
 - 16 v. Whether Defendant knew about the September 2018 Data Breach before it
17 was announced to the public and Defendant failed to timely notify the
18 public of the September 2018 Data Breach;
 - 19 vi. Whether Defendant's conduct violated Cal. Civ. Code § 1750, *et seq.*;
 - 20 vii. Whether Defendant's conduct was an unlawful or unfair business practice
21 under Cal. Bus. & Prof. Code § 17200, *et seq.*;
 - 22 viii. Whether Defendant's conduct violated the Consumer Records Act, Cal.
23 Civ. Code § 1798.80 *et seq.*;
 - 24 ix. Whether Defendant's conduct violated the Online Privacy Protection Act,
25 Cal. Bus. & Prof. Code § 22575, *et seq.*,
 - 26 x. Whether Defendant's conduct violated § 5 of the Federal Trade
27 Commission Act, 15 U.S.C. § 45, *et seq.*,
- 28

- 1 xi. Whether Plaintiffs and the Class are entitled to equitable relief, including,
2 but not limited to, injunctive relief and restitution; and
3 xii. Whether Plaintiffs and the other Class members are entitled to actual,
4 statutory, or other forms of damages, and other monetary relief.

5 39. Similar or identical statutory and common law violations, business practices,
6 and injuries are involved. Individual questions, if any, pale by comparison, in both quantity
7 and quality, to the numerous common questions that dominate this action.

8 40. **Typicality:** Plaintiffs' claims are typical of the claims of the other members of
9 their respective classes because, among other things, Plaintiffs and the other Class members
10 were injured through the substantially uniform misconduct by Defendant. Plaintiffs are
11 advancing the same claims and legal theories on behalf of themselves and all other Class
12 members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and
13 those of other Class members arise from the same operative facts and are based on the same
14 legal theories.
15

16 41. **Adequacy of Representation:** Plaintiffs are adequate representatives of the
17 classes because their interests do not conflict with the interests of the other Class members they
18 seek to represent; they have retained counsel competent and experienced in complex class
19 action litigation and Plaintiffs will prosecute this action vigorously. The Class members'
20 interests will be fairly and adequately protected by Plaintiffs and their counsel.
21

22 42. **Superiority:** A class action is superior to any other available means for the fair
23 and efficient adjudication of this controversy, and no unusual difficulties are likely to be
24 encountered in the management of this matter as a class action. The damages, harm, or other
25 financial detriment suffered individually by Plaintiffs and the other members of their respective
26 classes are relatively small compared to the burden and expense that would be required to
27
28

1 litigate their claims on an individual basis against Defendant, making it impracticable for Class
2 members to individually seek redress for Defendant's wrongful conduct. Even if Class
3 members could afford individual litigation, the court system could not. Individualized litigation
4 would create a potential for inconsistent or contradictory judgments, and increase the delay
5 and expense to all parties and the court system. By contrast, the class action device presents
6 far fewer management difficulties and provides the benefits of single adjudication, economies
7 of scale, and comprehensive supervision by a single court.

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

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

- 16 a. Whether Class members' PII was accessed, compromised, or stolen in the
17 September 2018 Data Breach;
- 18 b. Whether (and when) Defendant knew about any security vulnerabilities that led
19 to the September 2018 Data Breach before they were announced to the public
20 and whether Defendant failed to timely notify the public of those vulnerabilities
21 and the September 2018 Data Breach;
- 22 c. Whether Defendant's conduct was an unlawful or unfair business practice under
23 Cal. Bus. & Prof. Code § 17200, *et seq.*;
- 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
- d. Whether Defendant’s representations that it would secure and protect the PII of Plaintiffs and members of the classes were facts that reasonable persons could be expected to rely upon when deciding whether to use Defendant’s services;
 - e. Whether Defendant misrepresented the safety of its many systems and services, specifically the security thereof, and its ability to safely store Plaintiffs’ and Class members’ PII;
 - f. Whether Defendant concealed crucial information about its inadequate data security measures from Plaintiffs and the Class;
 - g. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
 - h. Whether Defendant knew or should have known that it did not employ reasonable measures to keep Plaintiffs’ and Class members’ PII secure and prevent the loss or misuse of that information;
 - i. Whether Defendant 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;
 - j. Whether Defendant failed to provide timely notice of the September 2018 Data Breach in violation of California Civil Code § 1798.82;
 - k. Whether Defendant’s conduct violated Cal. Bus. & Prof. Code § 22575, *et seq.*;
 - l. Whether Defendant owed a duty to Plaintiffs and the Class to safeguard their PII and to implement adequate data security measures;
 - m. Whether Defendant breached that duty;

- 1 n. Whether Defendant failed to adhere to its posted privacy policy concerning the
2 care it would take to safeguard Plaintiffs’ and Class members’ PII in violation
3 of California Business and Professions Code § 22576;
- 4 o. Whether Defendant negligently and materially failed to adhere to its posted
5 privacy policy with respect to the extent of its disclosure of users’ data, in
6 violation of California Business and Professions Code § 22576;
- 7 p. Whether such representations were false with regard to storing and
8 safeguarding Class members’ PII; and
- 9 q. Whether such representations were material with regard to storing and
10 safeguarding Class members’ PII.
11

12 **CLAIMS ALLEGED ON BEHALF OF ALL CLASSES**

13 **First Claim for Relief**

14 **Violation of California’s Unfair Competition Law (“UCL”) – Unlawful Business
15 Practice (Cal. Bus. & Prof. Code § 17200, *et seq.*)**

16 45. Plaintiffs repeat, reallege, and incorporate by reference the allegations
17 contained in paragraphs 1 through 44 as though fully stated herein.

18 46. By reason of the conduct alleged herein, Defendant engaged in unlawful
19 practices within the meaning of the UCL. The conduct alleged herein is a “business practice”
20 within the meaning of the UCL.

21 47. Facebook represent that it would not disclose users’ PII without consent and/or
22 notice. Facebook further represented that it would utilize sufficient data security protocols and
23 mechanisms to protect users’ PII.
24

25 48. Defendant stored the PII of Plaintiffs and members of their respective Classes
26 in Defendant’s electronic and consumer information databases. Defendant falsely represented
27 to Plaintiffs and members of the Classes that the PII databases were secure and that class
28

1 members' PII would remain private. Defendant knew or should have known it did not employ
2 reasonable, industry standard, and appropriate security measures that complied "with federal
3 regulations" and that would have kept Plaintiffs' and the other Class members' PII secure and
4 prevented the loss or misuse of Plaintiffs' and the other class members' PII.

5 49. Even without these misrepresentations, Plaintiffs and Class members were
6 entitled to assume, and did assume Defendant would take appropriate measures to keep their
7 PII safe. Defendant did not disclose at any time that Plaintiffs' PII was vulnerable to hackers
8 because Defendant's data security measures were inadequate, and Defendant was the only one
9 in possession of that material information, which it had a duty to disclose. Defendant violated
10 the UCL by misrepresenting, both by affirmative conduct and by omission, the safety of its
11 many systems and services, specifically the security thereof, and its ability to safely store
12 Plaintiffs' and Class members' PII. Defendant also violated the UCL by failing to implement
13 reasonable and appropriate security measures or follow industry standards for data security,
14 and failing to comply with its own posted privacy policies. If Defendant had complied with
15 these legal requirements, Plaintiffs and the other Class members would not have suffered the
16 damages described herein.
17
18

19 50. Defendant's acts, omissions, and misrepresentations as alleged herein were
20 unlawful and in violation of, *inter alia*, Cal. Civ. Code § 1798.81.5(b), Section 5(a) of the
21 Federal Trade Commission Act, 15 U.S.C. § 45(a), Cal. Bus. & Prof. Code § 22576 (as a result
22 of Facebook failing to comply with its own posted privacy policies).

23 51. Plaintiffs and the Class members suffered injury in fact and lost money or
24 property as the result of Defendant's unlawful business practices.²¹ In particular, Plaintiffs'
25

26
27 ²¹ Plaintiffs recognize that this Court ruled out of pocket expenses and the risk of future harm
28 lacked standing. However, Plaintiffs have included all named representatives in the

1 and Class members' PII was taken and is in the hands of those who will use it for their own
2 advantage, or is being sold for value, making it clear that information is of tangible value;
3 hacked Facebook accounts and any accounts linked to their Facebook accounts; and other
4 similar harm, all as a result of the September 2018 Data Breach.

5 52. As a result of Defendant's unlawful business practices, violations of the UCL,
6 Plaintiffs and the Class members are entitled to restitution, disgorgement of wrongfully
7 obtained profits and injunctive relief.
8

9 **Second Claim for Relief**
10 **Violation of California's Unfair Competition Law ("UCL") – Unfair Business Practice**
11 **(Cal. Bus. & Prof. Code § 17200, *et seq.*)**

12 53. Plaintiffs repeat, reallege, and incorporate by reference the allegations
13 contained in paragraphs 1 through 44 as though fully stated herein.

14 54. By reason of the conduct alleged herein, Defendant engaged in unfair "business
15 practices" within the meaning of the UCL.

16 55. Defendant stored the PII of Plaintiffs and members of their respective Classes
17 in their electronic and consumer information databases. Defendant represented to Plaintiffs and
18 members of the classes that its PII databases were secure and that class members' PII would
19 remain private. Defendant engaged in unfair acts and business practices by representing that it
20 had safeguards that comply with federal regulations to protect PII."

21 56. Even without these misrepresentations, Plaintiffs and Class members were
22 entitled to, and did, assume Defendant would take appropriate measures to keep their PII safe.
23 Defendant did not disclose at any time that Plaintiffs' PII was vulnerable to hackers because
24 Defendant's data security measures were inadequate and outdated, and Defendant was the only
25 one in possession of that material information, which it had a duty to disclose.
26

27
28 _____
"unlawful" and "unfair" UCL causes of action to preserve this issue for appeal.

1 57. Defendant knew or should have known it did not employ reasonable measures
2 that would have kept Plaintiffs' and the other Class members' PII secure and prevented the
3 loss or misuse of Plaintiffs' and the other Class members' PII.

4 58. Defendant violated the UCL by misrepresenting, both by affirmative conduct
5 and by omission, the security of its many systems and services, and its ability to safely store
6 Plaintiffs' and Class members' PII. Defendant also violated the UCL by failing to implement
7 and maintain reasonable security procedures and practices appropriate to protect all class
8 members' PII. If Defendant followed the industry standards and legal requirements, Plaintiffs
9 and the Class would not have suffered the damages alleged herein.
10

11 59. Defendant also violated its commitment to maintain the confidentiality and
12 security of the PII of Plaintiffs and their respective Classes, and failed to comply with its own
13 policies and applicable laws, regulations, and industry standards relating to data security.

14 60. **Defendant engaged in unfair business practices under the "balancing test."**
15 The harm caused by Defendant's actions and omissions, as described in detail above, greatly
16 outweigh any perceived utility. Indeed, Defendant's failure to follow basic data security
17 protocols and misrepresentations to consumers about Defendant's data security cannot be said
18 to have had any utility at all.
19

20 61. **Defendant engaged in unfair business practices under the "tethering test."**
21 Defendant's actions and omissions, as described in detail above, violated fundamental public
22 policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 ("The
23 Legislature declares that ... all individuals have a right of privacy in information pertaining to
24 them.... The increasing use of computers ... has greatly magnified the potential risk to
25 individual privacy that can occur from the maintenance of personal information."); Cal. Civ.
26 Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information
27
28

1 about California residents is protected.”); Cal. Bus. & Prof. Code § 22578 (“It is the intent of
2 the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of
3 statewide concern.”) Defendant’s acts and omissions, and the injuries caused by them are thus
4 “comparable to or the same as a violation of the law ...” *Cel-Tech Communications, Inc. v.*
5 *Los Angeles Cellular Telephone Co.* (1999) 20 Cal.4th 163, 187.

6 **62. Defendant engaged in unfair business practices under the “FTC test.”** The
7 harm caused by Defendant’s actions and omissions, as described in detail above, is substantial
8 in that it affects approximately 50 million Class members and has caused those persons to
9 suffer actual harms. Such harms include a substantial risk of identity theft, disclosure of Class
10 members’ PII to third parties without their consent, diminution in value of their PII,
11 consequential out of pocket losses for procuring credit freeze or protection services, identity
12 theft monitoring, and other expenses relating to identity theft losses or protective measures.
13 This harm continues given the fact that Class members’ PII remains in Defendant’s possession,
14 without adequate protection, and is also in the hands of those who obtained it without their
15 consent. Defendant’s actions and omissions violated, *inter alia*, Section 5(a) of the Federal
16 Trade Commission Act, 15 U.S.C. § 45. *See, e.g., F.T.C. v. Wyndham Worldwide Corp.*, 10 F.
17 Supp. 3d 602, 613 (D.N.J. 2014), *aff’d*, 799 F.3d 236 (3d Cir. 2015); *In re LabMD, Inc.*, FTC
18 Docket No. 9357, FTC File No. 102-3099 (July 28, 2016) (failure to employ reasonable and
19 appropriate measures to secure personal information collected violated § 5(a) of FTC Act); *In*
20 *re BJ’s Wholesale Club, Inc.*, FTC Docket No. C-4148, FTC File No. 042-3160 (Sept. 20,
21 2005) (same); *In re CardSystems Solutions, Inc.*, FTC Docket No. C-4168, FTC File No. 052-
22 3148 (Sept. 5, 2006) (same); *see also United States v. ChoicePoint, Inc.*, Civil Action No. 1:06-
23 cv-0198-JTC (N.D. Ga. Oct. 14, 2009) (“failure to establish and implement, and thereafter
24 maintain, a comprehensive information security program that is reasonably designed to protect
25
26
27
28

1 the security, confidentiality, and integrity of personal information collected from or about
2 consumers” violates § 5(a) of FTC Act); 15 U.S.C. § 45(n) (defining “unfair acts or practices”
3 as those that “cause[] or [are] likely to cause substantial injury to consumers which [are] not
4 reasonably avoidable by consumers themselves and not outweighed by countervailing benefits
5 to consumers or to competition.”).

6 63. Plaintiffs and the Class members suffered injury in fact and lost money or
7 property as the result of Defendant’s unfair business practices. In particular, Plaintiffs and
8 Class members have suffered from hacked Facebook accounts and any accounts linked to their
9 Facebook accounts; and other similar harm, all as a result of the September 2018 Data Breach.
10 In addition, their PII was taken and is in the hands of those who will use it for their own
11 advantage, or is being sold for value, making it clear that the hacked information is of tangible
12 value. Plaintiffs and Class members have also suffered consequential out of pocket losses for
13 procuring credit freeze or protection services, identity theft monitoring, and other expenses
14 relating to identity theft losses or protective measures.
15

16 64. As a result of Defendant’s unfair business practices, violations of the UCL,
17 Plaintiffs and the Class members are entitled to restitution, disgorgement of wrongfully
18 obtained profits, and injunctive relief.
19

20 **Third Claim for Relief**
21 **Deceit by Concealment — Cal. Civil Code §§ 1709, 1710**

22 65. Plaintiffs repeat, reallege, and incorporate by reference the allegations
23 contained in paragraphs 1 through 44 as though fully stated herein.

24 66. As alleged above, Defendant knew its data security measures were grossly
25 inadequate by, at the absolute latest, March 2018 when the Cambridge Analytica matter came
26 to light, exposing Facebook’s lax and inadequate approach to data security. At that time,
27
28

1 Facebook was on notice that its systems were extremely vulnerable to attack, facts Defendant
2 already knew given its previous exposures and security problems.

3 67. In response to all of these facts, Defendant chose to do nothing to protect
4 Plaintiffs and the Class or warn them about the security problems and, instead, openly
5 represented to Congress and foreign governments that Facebook was dedicated to the highest
6 and most advance security practices and protocols.

7 68. Defendant had an obligation to disclose to all class members that their Facebook
8 accounts and PII were an easy target for hackers and Defendant was not implementing
9 measures to protect them.
10

11 69. Defendant did not do these things. Instead, Defendants willfully deceived
12 Plaintiffs and the Class by concealing the true facts concerning their data security, which
13 Defendants were obligated to, and had a duty to, disclose. Additionally, Facebook made
14 numerous representations following the prior exposures to ensure users that their PII and other
15 data was safe, and Facebook was dedicated to maintaining that security.
16

17 70. Had Defendant disclosed the true facts about its poor data security, Plaintiffs
18 and the Class would have taken measures to protect themselves. Plaintiffs and the Class
19 justifiably relied on Defendant to provide accurate and complete information about
20 Defendant's data security, and Defendant did not.

21 71. Alternatively, given the security holes in Defendant's services and Defendant's
22 refusal to take measures to detect those holes, much less fix them, Defendant simply should
23 have shut down their current service. Independent of any representations made by Defendant,
24 Plaintiffs and the Class justifiably relied on Defendant to provide a service with at least
25 minimally adequate security measures and justifiably relied on Defendant to disclose facts
26 undermining that reliance.
27
28

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

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

13 80. By being entrusted by Plaintiffs and the Class to safeguard their PII, Defendant
14 had a special relationship with Plaintiffs and the Class. Plaintiffs and the Class signed up for
15 Defendant's services and agreed to provide their PII with the understanding that Defendant
16 would take appropriate measures to protect it, and would inform Plaintiffs and the Class of any
17 breaches or other security concerns that might call for action by Plaintiffs and the Class. But,
18 Defendant did not. Defendant not only knew its data security was inadequate, Defendant also
19 knew it didn't have the tools to detect and document intrusions or exfiltration of PII. Defendant
20 is morally culpable, given its repeated security breaches, wholly inadequate safeguards, and
21 refusal to notify Plaintiffs and the Class of breaches or security vulnerabilities,
22
23
24

25 81. Defendant breached its duty to exercise reasonable care in safeguarding and
26 protecting Plaintiffs' and the Class members' PII by failing to adopt, implement, and maintain
27
28

1 adequate security measures to safeguard that information, despite repeated failures and
2 intrusions, and allowing unauthorized access to Plaintiffs' and the other Class members' PII.

3 82. Defendant's failure to comply with industry and federal regulations further
4 evidences Defendant's negligence in failing to exercise reasonable care in safeguarding and
5 protecting Plaintiffs' and the Class members' PII.

6 83. Defendant's breaches of these duties were not merely isolated incidents or small
7 mishaps. Rather, the breaches of the duties set forth above resulted from a long-term company-
8 wide refusal by Defendant to acknowledge and correct serious and ongoing data security
9 problems.
10

11 84. But for Defendant's wrongful and negligent breach of its duties owed to
12 Plaintiffs and the Class, their PII would not have been compromised, stolen, and viewed by
13 unauthorized persons. Defendant's negligence was a direct and legal cause of the theft of the
14 PII of Plaintiffs and the Class and all resulting damages.

15 85. The injury and harm suffered by Plaintiffs and the Class members was the
16 reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding
17 and protecting Plaintiffs' and the other class members' PII. Defendant knew its systems and
18 technologies for processing and securing the PII of Plaintiffs and the Class had numerous
19 security vulnerabilities.
20

21 86. As a result of this misconduct by Defendant, the PII of Plaintiffs and the Class
22 were compromised, placing them at a greater risk of identity theft and subjecting them to
23 identity theft, and their PII was disclosed to third parties without their consent. Plaintiffs and
24 Class members also suffered diminution in value of their PII in that it is now easily available
25 to hackers on the Dark Web. Plaintiffs and the Class have also suffered consequential out of
26
27
28

1 pocket losses for procuring credit freeze or protection services, identity theft monitoring, and
2 other expenses relating to identity theft losses or protective measures.

3 87. Defendant’s misconduct as alleged herein is malice or oppression under Civil
4 Code § 3294(c)(1) and (2) in that it was despicable conduct carried on by Defendant with a
5 willful and conscious disregard of the rights or safety of Plaintiffs and the Class and despicable
6 conduct that has subjected Plaintiffs and the Class to cruel and unjust hardship in conscious
7 disregard of their rights. As a result, Plaintiffs and the Class are entitled to punitive damages
8 against Defendants under Civil Code § 3294(a).
9

10 **ADDITIONAL CLAIMS ALLEGED ON BEHALF OF THE CALIFORNIA**
11 **SUBCLASS ONLY**

12 **Fifth Claim for Relief**
13 **Violation of California’s Customer Records Act – Inadequate Security**
14 **(Cal. Civ. Code § 1798.81.5)**

15 88. Plaintiff Echavarria repeats, realleges, and incorporates by reference the
16 allegations contained in paragraphs 1 through 44 as though fully stated herein.

17 89. Plaintiff Echavarria brings this claim on behalf of the California Subclass.

18 90. California Civil Code section 1798.80, *et seq.*, known as the “Customer
19 Records Act” (“CRA”) was enacted to “encourage business that own, license, or maintain
20 personal information about Californians to provide reasonable security for that information.”
21 Cal. Civ. Code § 1798.81.5(a)(1).

22 91. Section 1798.81.5, subdivision (b) of the CRA requires any business that
23 “owns, licenses, or maintains personal information about a California resident” to “implement
24 and maintain reasonable security procedures and practices appropriate to the nature of the
25 information,” and “to protect the personal information from unauthorized access, destruction,
26 use, modification, or disclosure.” Section 1798.81.5, subdivision (d)(1)(B) defines “personal
27 information” as including “A username or email address in combination with a password or
28

1 security question and answer that would permit access to an online account.” “Personal
2 information” also includes an individual’s first name or first initial in combination with a social
3 security number, driver’s license number, account number or credit or debit card number and
4 access code, medical information, or health insurance information. Cal. Civ. Code §
5 1798.82(h).

6 92. Defendant is a business that owns, licenses, or maintains personal information
7 about California residents. As alleged in detail above, Defendant failed to implement and
8 maintain reasonable security procedures and practices appropriate to the nature of the
9 information, and protect the personal information from unauthorized access, destruction, use,
10 modification, or disclosure, resulting in the September 2018 Data Breach.

11 93. As the direct and legal result of Defendant’s violation of section 1798.81.5,
12 Plaintiff Echavarria and the members of the California subclass were harmed because their PII
13 was compromised, placing them at a greater risk of identity theft and their PII disclosed to third
14 parties without their consent. Plaintiff Echavarria and Class members also suffered diminution
15 in value of their PII in that it is now easily available to hackers on the Dark Web. Plaintiff
16 Echavarria and the California subclass have also suffered consequential out of pocket losses
17 for procuring credit freeze or protection services, identity theft monitoring, and other expenses
18 relating to identity theft losses or protective measures. The California subclass members are
19 further damaged as their PII remains Defendant’s possession, without adequate protection, and
20 is also in the hands of those who obtained it without their consent.
21

22 94. Plaintiff Echavarria and the California subclass seek all remedies available
23 under Cal. Civ. Code § 1798.84, including, but not limited to damages suffered by Plaintiffs
24 and the other class members as alleged above and equitable relief.
25
26
27
28

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

3 (h) Awarding Plaintiffs and the Class members punitive damages;

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

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

8 (k) Granting such other relief as the Court deems just and proper.
9

10 **JURY TRIAL DEMANDED**

11 Plaintiffs demand a trial by jury of all claims in this Class Action Complaint so triable.
12

13 Dated: September 28, 2018

/s/ Joshua H. Watson
JOSHUA H. WATSON

Attorney for Plaintiffs