Clayeo C. Arnold, California SBN 65070
carnold@justice4you.com
Joshua H. Watson, California SBN 238058
jwatson@justice4you.com
CLAYEO C. ARNOLD, A PROFESSIONAL LAW CORPORATION
865 Howe Avenue
Sacramento, California 95825
T: 916-777-7777
F: 916-924-1829

MORGAN & MORGAN COMPLEX LITIGATION GROUP
John A. Yanchunis (Pro Hac Vice Forthcoming)
jyanchunis@ForThePeople.com
Ryan J. McGee (Pro Hac Vice Forthcoming)
rmcgee@ForThePeople.com
Jean S. Martin (Pro Hac Vice Forthcoming)
jeanmartin@ForThePeople.com
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: 813/223-5505
813/223-5402 (fax)

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

CARLA ECHAVARRIA, an individual and California Resident, and DERRICK 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

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

SUMMARY OF THE CASE

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

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

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

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

JURISDICTION AND VENUE

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

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

PARTIES

A. Plaintiffs

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

8. Plaintiff Derrick Walker ("Walker") is a resident and citizen of Virginia. Plaintiff Walker opened a Facebook account and used it for years, entrusting Facebook with

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

B. Defendant

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

FACTUAL BACKGROUND

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

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

11. Facebook's Terms of Service state that the Facebook user is the owner of all of their data. Facebook's representation to Plaintiffs and Class Members that "Protecting people's information is at the heart of everything we do"[1] was in fact a misrepresentation, and one which Plaintiff and Class Members relied upon.

12. Facebook represents to its users that: "you have control over who sees what you share on Facebook."[2] Facebook represents to its users that: "We have top-rate security

[1] Matthew Rosenberg, Nicholas Confessore, and Carole Cadwalladr, *How Trump Consultants Exploited the 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 August 30, 2018).

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

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

13. At all relevant times, Facebook has maintained a Data Use Policy on its website. That Data Use Policy advised Facebook users, in part:

> Granting us permission to use your information not only allows us to provide Facebook as it exists today, but it also allows us to provide you with innovative features and services we develop in the future that use the information we receive about you in new ways. While you are allowing us to use the information we receive about you, you always own all of your information. ***Your trust is important to us, which is why we don't share information we receive about you with others unless we have:***
>
> - ***received your permission***
> - ***given you notice***, such as by telling you about it in this policy; or
> - removed your name and any other personally identifying information from it.

(Emphases added).[7]

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

---

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

on Facebook's representations for the security of their PII in using Facebook and posting PII on Facebook.

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

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

- Device attributes: information such as the operating system, hardware and software versions, battery level, signal strength, available storage space, browser type, app and file names and types, and plugins.
- Device operations: information about operations and behaviors performed on the device, such as whether a window is foregrounded or backgrounded, or mouse movements (which can help distinguish humans from bots).
- Identifiers: unique identifiers, device IDs, and other identifiers, such as from games, apps or accounts people use, and Family Device IDs (or other identifiers unique to Facebook Company Products associated with the same device or account).
- Device signals: Bluetooth signals, and information about nearby Wi-Fi access points, beacons, and cell towers.
- Data from device settings: information users allow us to receive through device settings people turn on, such as access to their GPS location, camera, or photos.
- Network and connections: information such as the name of users' mobile operator or ISP, language, time zone, mobile phone number, IP address, connection speed and, in some cases, information about other devices that are nearby or on users' network, so we can do things like help people 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.

entities—Facebook's lax approach to data security resulted in a data breach affected 50 million users (the "September 2018 Data Breach").

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

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

B. PII is Very Valuable on the Black Market

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

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

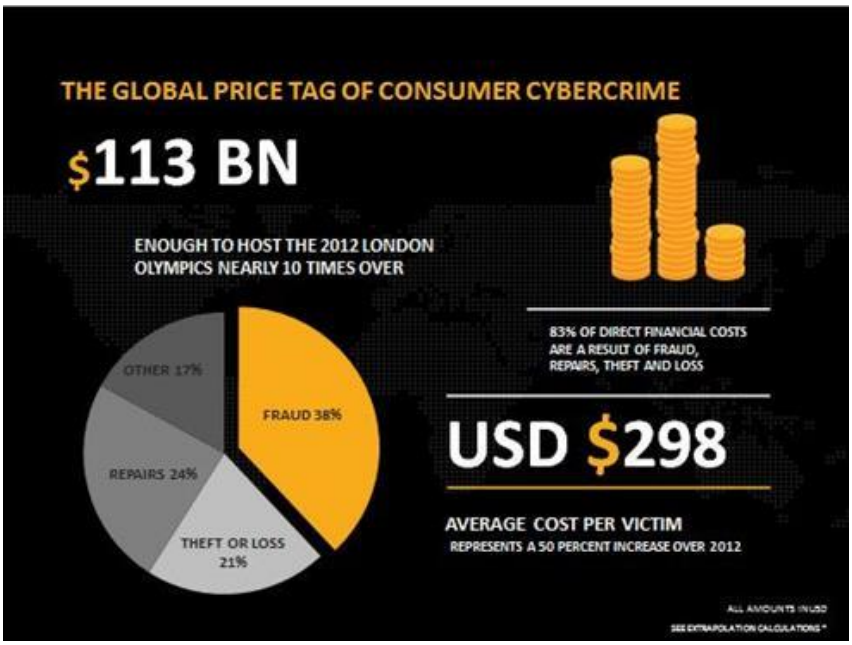
> In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they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

[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 (last visited August 30, 2018)

[12] *Id.*

> example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.[13]

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



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

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

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

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

26. In addition to PII, a hacked Facebook account can be very valuable to cyber criminals. Since Facebook accounts are linked to myriad accounts, a hacked Facebook account could open up a number of other accounts to an attacker.

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

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

27. On September 28, 2018, Facebook announced the "previously unreported attack on its network," exposing the PII of "nearly 50 million users."[15]

28. Facebook claims it discovered the vulnerability "earlier this week," that Facebook entirely fixed the vulnerability, and law enforcement was notified.[16]

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

30. The vulnerability Facebook disclosed was a bug in its site's "view as" feature, which permits users to view their profiles posing as someone else, which, ironically, was built in to give users more control over their privacy.[18]

31. In a conference call, Guy Rosen, a vice president of product management at Facebook, admitted the September 2018 Data Breach was "complex," and "leveraged three separate bugs in Facebook's code that, once compounded, provided widespread access to user accounts."[19]

32. Senator Mark Warner, a Democrat from Virginia, stated "This is another sobering indicator that Congress needs to step up and take action to protect the privacy and

---

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

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

[17] Id.

[18] Id.

[19] Id.

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

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

CLASS ACTION ALLEGATIONS

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

A. The United States Class

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

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

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

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

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

[20] Id.

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

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

i. Whether Defendant represented to the Class that it would safeguard Class members' PII;

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

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

iv. Whether Class members' PII was accessed, compromised, or stolen in the September 2018 Data Breach;

v. Whether Defendant knew about the September 2018 Data Breach before it was announced to the public and Defendant failed to timely notify the public of the September 2018 Data Breach;

vi. Whether Defendant's conduct violated Cal. Civ. Code § 1750, *et seq.*;

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

viii. Whether Defendant's conduct violated the Consumer Records Act, Cal. Civ. Code § 1798.80 *et seq.*;

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

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

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

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

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

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

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

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

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

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

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

a. Whether Class members' PII was accessed, compromised, or stolen in the September 2018 Data Breach;

b. Whether (and when) Defendant knew about any security vulnerabilities that led to the September 2018 Data Breach before they were announced to the public and whether Defendant failed to timely notify the public of those vulnerabilities and the September 2018 Data Breach;

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

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;

n. Whether Defendant failed to adhere to its posted privacy policy concerning the care it would take to safeguard Plaintiffs' and Class members' PII in violation of California Business and Professions Code § 22576;

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

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

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

CLAIMS ALLEGED ON BEHALF OF ALL CLASSES

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

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

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

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

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

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

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

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

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

[21] Plaintiffs recognize that this Court ruled out of pocket expenses and the risk of future harm were not sufficient to confer standing under the UCL, and thus certain named plaintiffs lacked standing. However, Plaintiffs have included all named representatives in the

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

74. As a result of this deceit by Defendant, it is liable under Cal. Civil Code § 1709 for "any damage which [Plaintiffs and the Class] thereby suffer[]."

75. As a result of this deceit by Defendant, the PII of Plaintiffs and the Class were compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their PII was disclosed to third parties without their consent. Plaintiffs and Class members also suffered diminution in value of their PII in that it is now easily available to hackers on the Dark Web. Plaintiffs and the Class have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

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

Fourth Claim for Relief
Negligence

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

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

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

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

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

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

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

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

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

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

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

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

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

ADDITIONAL CLAIMS ALLEGED ON BEHALF OF THE CALIFORNIA SUBCLASS ONLY

Fifth Claim for Relief
Violation of California's Customer Records Act – Inadequate Security
(Cal. Civ. Code § 1798.81.5)

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

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

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

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

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

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

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

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

95. Defendant's misconduct as alleged herein is fraud under Civil Code § 3294(c)(3) in that it was deceit or concealment of a material fact known to the Defendant conducted with the intent on the part of Defendant of depriving Plaintiffs and the Class of "legal rights or otherwise causing injury." In addition, Defendant's misconduct as alleged herein is malice or oppression under Civil Code § 3294(c)(1) and (2) in that it was despicable conduct carried on by Defendant with a willful and conscious disregard of the rights or safety of Plaintiff and the Class and despicable conduct that has subjected Plaintiff and the Class to cruel and unjust hardship in conscious disregard of their rights. As a result, Plaintiff and the Class are entitled to punitive damages against Defendant under Civil Code § 3294(a).

PRAYER FOR RELIEF

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

(a) Certifying the United States Class and California Subclass, and appointing Plaintiffs as Class and Subclass Representatives;

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

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

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

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

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

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

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

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

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

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

JURY TRIAL DEMANDED

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

Dated: September 28, 2018

/s/ *Joshua H. Watson*
JOSHUA H. WATSON

Attorney for Plaintiffs