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
Jonathan B. Cohen
jcohen@ForThePeople.com
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
T: 813-223-5505
F: 813-223-5402

MORGAN & MORGAN COMPLEX LITIGATION GROUP
Jean S. Martin (Pro Hac Vice Forthcoming)
jeanmartin@ForThePeople.com
2018 Eastwood Road, Suite 225
Wilmington, NC 28403
T: 813-559-4908
F: 813-222-4795

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

MATT MATIC, an individual and California Resident, and ZAK HARRIS, an individual and Florida Resident,

Plaintiffs,

v.

GOOGLE, LLC, and ALPHABET, INC.,

Defendants

CASE NO. 5:18-cv-06164-EJD

FIRST AMENDED CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

(1) UCL – Unlawful Business Practice
(2) UCL – Unfair Business Practice
(3) Negligence
(4) Invasion of Privacy
(5) Breach of Confidence
(6) California's Customer Records Act

TABLE OF CONTENTS

For their Amended Class Action Complaint, Plaintiffs Matt Matic and Zak Harris, on behalf of themselves and all others similarly situated, allege the following against Defendant Google, LLC ("Google") and Defendant Alphabet, Inc. ("Alphabet"), 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. Launched in June 2011, Google+ (or Google Plus) is a social network owned and operated by Google for consumers with Google accounts. Google+ facilitates the sharing of information, photographs, weblinks, conversations, and other shared content similar in many respects to the Facebook news feed or Twitter stream.

2. Google+ was created as Google's answer and rival to Facebook, but is widely seen as one of Google's biggest failures.[1]

3. As part of the sign up process and as a consequence of interacting with the network, users of Google+ 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 "Personal Information."

4. When you add a contact to your Google+ account, you assign that person to one or more "circles", which is a way of categorizing or organizing contacts.

5. Google+ users determine privacy settings for content, allowing content to be shared with the public or with only those in designated circles.

6. This case involves two data leaks Google and Alphabet announced: the first on October 8, 2018, wherein the Personal Information of up to 500,000 users was exposed (the "First Data Leak"); and the second on December 10, 2018, wherein the Personal Information of up to 52.5 million users was exposed (the "Second Data Leak") (collectively,

[1] THE WALL STREET JOURNAL, *Google Exposed User Data, Feared Repercussions of Disclosing to Public* (October 8, 2018), https://www.wsj.com/articles/google-exposed-user-data-feared-repercussions-of-disclosing-to-public-1539017194? (last visited October 8, 2018).

the "Data Leaks"). Upon information and belief, both Data Breaches resulted from the same software glitch that gave third-party application developers access to private Google+ profile data between 2015 and March 2018.

7. While this information was supposed to be protected, and shared only with expressed permissions and limitations, Defendants allowed third-party application developers to improperly collect the Personal Information of up to 53 million Google+ users.

8. This Amended Class Action Complaint is filed on behalf of all persons in the United States, described more fully in the following sections, whose Personal Information was compromised in the Data Breaches.

JURISDICTION AND VENUE

9. 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. The Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

10. Venue is proper under 28 U.S.C. § 1391(c) because Defendants are corporations that do business in and are subject to personal jurisdiction in this District. Venue is also proper 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 Defendants' governance and management personnel that led to the data leak and the decision not to disclose the leak. Further, Google's Terms of Service governing users in the United States provides for venue in the Northern District of California for all claims arising out of Plaintiffs' relationship with Google.

PARTIES

A. Plaintiffs

11. Plaintiff Matt Matic is a resident and citizen of California. Plaintiff Matic opened a Google+ account and has used it for many years. Plaintiff Matic also uses a Gmail

account for his primary email. Through the opening and use of these accounts, Plaintiff Harris has entrusted Google with his Personal Information for all relevant time periods.

12. Plaintiff Zak Harris is a resident and citizen of Florida. Plaintiff Harris opened a Google+ account and used it since the inception of the platform. Plaintiff Harris also uses a Gmail account for email. Through the opening and use of these accounts, Plaintiff Harris has entrusted Google with his Personal Information for all relevant time periods.

B. Defendants

13. Defendant Google, LLC ("Google"), is a Delaware corporation with its principal headquarters in Mountain View, California.

14. Defendant Alphabet, Inc. ("Alphabet"), is a Delaware corporation with its principal headquarters in Mountain View, California. Alphabet is a public holding company formed in a corporate reorganization by Google. Through the corporate restructuring, Defendant Google is now a direct, wholly owned subsidiary of Defendant Alphabet.[2]

FACTUAL BACKGROUND

A. Google's Inadequate Data Security Allows the Massive Leak of Users' Personal Information

15. Google's Terms of Service make it clear that Google collects information from its users.[3] But at all relevant times, Google has maintained a Privacy Policy advising its users that: "When you use our services, you're trusting us with your information. We understand this is a big responsibility and work hard to protect your information and put you in control."[4] Further, Google represents that "We'll share Personal Information outside of Google when we have your consent."[5]

---

[2] Google, Inc., Form 8-K, U.S. Securities and Exchange Commission (August 10, 2015), https://www.sec.gov/Archives/edgar/data/1288776/000128877615000039/a20150810form8-k.htm (last visited October 8, 2018).

[3] Google, *Terms of Service* (October 25, 2017), https://policies.google.com/terms?hl=en&gl=ZZ (last visited October 8, 2018).

[4] Google, *Privacy Policy* (May 25, 2018) (emphasis added), https://policies.google.com/privacy (last visited October 8, 2018).

[5] *Id.* (emphasis added).

16. Google represents to its users that:

a. "You have choices regarding the information we collect and how it's used."[6]

b. "We'll ask for your consent before using your information for a purpose that isn't covered in this Privacy Policy."[7]

c. "We'll ask for your explicit consent to share any sensitive Personal Information."[8]

17. And importantly for the Data Breaches, Google represents to its users they can "[c]ontrol whom you share information with through your account on Google+."[9]

18. Despite these representations, Google's lax approach to data security resulted in the Data Leaks affecting approximately 53 million Google+ users over a period of at least 3 years (the "2018 Data Leaks").

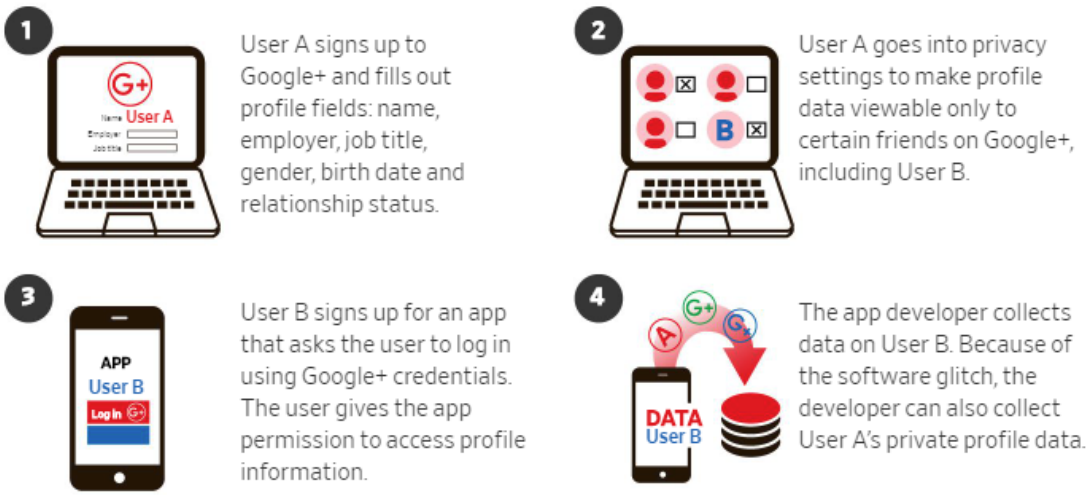
19. On October 8, 2018, Alphabet announced that it would be permanently shutting down the consumer functionality of Google+.[10] Along with this announcement, Alphabet disclosed that a "software glitch" had allowed outside application (also "app") vendors access to private Google+ profile data between 2015 and March 2018.

20. Google+ users may allow third party applications to access their private profile data. A "glitch" or "bug" in the Application Program Interfaces ("API") allowed the third party app to access the personal profile data of other Google+ users within the authorized user's circles.

---

[6] *Id.*
[7] *Id.*
[8] *Id.* (emphasis added).
[9] *Id.*
[10] THE WALL STREET JOURNAL, *Google Exposed User Data, Feared Repercussions of Disclosing to Public, supra* fn. 1.

21. The access allowed through this "glitch" is shown in the following illustration[11]:



22. Immediately, the First Data Leak drew comparisons to Facebook's leak of user information to Cambridge Analytica and other third party app developers.[12]

23. Given that Google+ was launched to challenge Facebook, the recent data security incidents suffered by Facebook users should have made Defendants more sensitive to the necessary protection of Google+ users' data. Instead, Defendants allowed this vulnerability for the First Data Leak in its system to endure for nearly 3 years, all the while leaking private information to unauthorized third parties.

24. Worse, after discovery of this vulnerability in the Google+ platform, Defendants kept silent for at least 7 months, making a calculated decision not to inform users that their Personal Information was compromised, further compromising the privacy of consumers' information and exposing them to risk of identity theft or worse.

25. Defendants advised that at least 438 third party applications may have used the API related to the First Data Leak and been allowed unauthorized access to Google+ users' data for nearly 3 years.[13]

---

[11] *Id.*

[12] *Id.* See also, https://www.washingtonpost.com/news/the-switch/wp/2018/04/04/facebook-said-the-personal-data-of-most-its-2-billion-users-has-been-collected-and-shared-with-outsiders/?utm_term=.57902e5f3d98 (last visited October 8, 2018).

26. Because the API logs are designed to keep historical data for only 2 weeks, Defendants were unable to tell exactly how many users may have had their information compromised during this 3 year period.[14]

27. Although Defendants initially reported that only up to 500,000 users were affected, Plaintiffs' gravest concerns proved true when Defendants announced the Second Data Leak, which concerned similar-if-not-identical API, and exposed the Personal Information of approximately 52.5 million Google+ users, bringing the total to 53 million Google+ users.[15]

28. Although Defendants represent that the Second Data Leak existed from November 7, 2018, through November 13, 2018, Defendants provide few details and still intend to operate the clearly bug-ridden and unsecure Google+ platform until April 2019.[16]

29. This case involves the absolute and intentional disregard with which Defendants have chosen to treat the Personal Information of users who utilize the Google+ social media platform. While this information was supposed to be protected and shared only with expressed permissions, Defendants, without authorization, exposed that information to third parties through lax and non-existent data safety and security policies and protocols.

B. Defendants Make A Business Decision Not To Disclose The First Data Leak

30. Even more serious and alarming, when Alphabet announced the First Data Leak, it made the startling revelation that they had discovered and "fixed" the security vulnerability in March 2018, an astonishing 7 months before the announcement.[17]

31. It has been reported that, faced with the news of this massive First Data Leak, Defendants made a calculated business decision, with the knowledge of Chief Executive

---

[13] ZD Net, *Google Shuts Down Google+ After API Bug Exposed Details For Over 500,000 Users* (October 8, 2018),https://www.zdnet.com/article/google-shuts-down-google-after-api-bug-exposed-details-for-over-500000-users/ (last visited October 8, 2018).

[14] *Id*.

[15] Statt and Brandom, *Google will shut down Google+ four months early after second data leak* (Dec. 10, 2018)https://www.theverge.com/platform/amp/2018/12/10/18134541/google-plus-privacy-api-data-leak-developers

[16] *Id.*

[17] THE WALL STREET JOURNAL, *Google Exposed User Data, Feared Repercussions of Disclosing to Public, supra* fn. 1.

Sundar Pichai, that disclosure of the First Data Leak might invite "regulatory interest" similar to what Facebook faced in the wake of the Cambridge Analytica debacle.[18]

32. Incredibly, Defendants chose to protect themselves from potential governmental inquiry rather than protect the Personal Information of its users and advise them that their Personal Information had been exposed in the First Data Leak to unauthorized third parties.

33. Defendants withheld the information of the First Data Leak from its users and the public until it made the decision to shut down the Google+ service for consumers in August 2019—approximately 10 months following the First Data Leak announcement.

34. In every turn, Defendants put their own business interests ahead of the privacy interests of Google+ users causing harm to Plaintiffs and Class members.

C. Defendants Announce the Second Data Leak

35. In the wake of the increased attention from the First Data Leak in October 2018, Defendants still operated the Google+ service, continuing to collect users' Personal Information, with plans to shut the Google+ service down in August 2019.

36. Approximately one month following the First Data Leak, Defendants permitted the Second Data Leak to persist from November 7, 2018, through November 13, 2018, when Defendants allegedly identified and fixed vulnerabilities that again permitted unauthorized third parties to access and aggregate users' Personal Information.[19]

37. This Second Data Leak, however, resulted in the exposure and dissemination of the Personal Information of approximately 52.5 million Google+ users—an approximate increase of 10,400% of effected Google+ users.

38. The Second Data Leak involved names, email addresses, occupations, ages, and other Personal Information, and was exposed to unauthorized third parties, despite users setting their accounts to private and explicitly denying Defendants the permission to share that Personal Information with unauthorized third parties.[20]

---

[18] *Id*.
[19] Statton and Brandom, *supra*, n.16
[20] Statton and Brandom, *supra* n.16

D. Personal Information is Very Valuable on the Black Market

39. The types of information compromised in the 2018 Data Leaks are highly valuable to identity thieves. The names, email addresses, occupation, birthdates, gender, nicknames, and other valuable Personal Information can all be used to gain access to a variety of existing accounts and websites.

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

> In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.[21]

41. 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.

[21] 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.

42. The problems associated with identity theft are exacerbated by the fact that many identity thieves will wait years before attempting to use the Personal Information 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.

43. Once stolen, Personal Information 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 Personal Information.[22] Websites appear and disappear quickly, making it a very dynamic environment.

44. Once someone buys Personal Information, it is then used to gain access to different areas of the victim's digital life, including bank accounts, social media, and credit

[22] 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.

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.

CLASS ACTION ALLEGATIONS

45. 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 in the United States who registered for Google+ accounts and whose Personal Information was accessed, compromised, or obtained from Google by third party applications without authorization or in excess of authorization as a result of the 2018 Data Leaks.

46. In addition, Plaintiff Matic brings this action on behalf of a California subclass defined as:

> All persons in California who registered for Google accounts and whose Personal Information was accessed, compromised, or obtained from Google by third party applications without authorization or in excess of authorization as a result of the 2018 Data Leaks.

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

48. **Numerosity:** The members of each Class are so numerous that joinder of all members of any Class would be impracticable. Defendants have indicated that at least 500,000 people had their Google+ accounts compromised as a result of the First Data Leak, and as many as 52,500,000 people had their Google+ accounts compromised as a result of the Second Data Leak. The identity of these Google+ users can be determined through records and documents maintained by Defendants.

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

i. Whether Defendants represented to the Class that it would safeguard Class members' Personal Information;

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

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

iv. Whether third parties improperly obtained Plaintiffs' and Class members' Personal Information without authorization or in excess of any authorization;

v. Whether Defendants were aware of other third parties' collection of Plaintiffs' and Class members' Personal Information without authorization or in excess of any authorization;

vi. Whether Defendants knew about the First Data Leak before it was announced to the public and Defendants failed to timely notify the public of the First Data Leak;

vii. Whether Defendants knew about the Second Data Leak before it was announced to the public and Defendants failed to timely notify the public of the Second Data Leak;

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

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

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

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

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

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

50. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs individually and on behalf of the members of the class. 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.

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

52. **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.

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

54. Further, Defendants 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.

55. 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' Personal Information was improperly obtained by third parties;

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

c. Whether (and when) Defendants knew about any security vulnerabilities that led to the Second Data Leak before they were announced to the public and whether Defendants failed to timely notify the public of those vulnerabilities and the Second Data Leak;

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

e. Whether Defendants' representations that it would secure and protect the Personal Information of Plaintiffs and members of the classes were facts that reasonable persons could be expected to rely upon when deciding whether to use Defendants' services;

f. Whether Defendants misrepresented the safety of its many systems and services, specifically the security thereof, and its ability to safely store Plaintiffs' and Class members' Personal Information;

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

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

i. Whether Defendants knew or should have known that they did not employ reasonable measures to keep Plaintiffs' and Class members' Personal

Information secure and prevent the unauthorized disclosure of that information;

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

k. Whether Defendants failed to provide timely notice of the First Data Leak in violation of California Civil Code § 1798.82;

l. Whether Defendants failed to provide timely notice of the Second Data Leak in violation of California Civil Code § 1798.82;

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

n. Whether Defendants owed a duty to Plaintiffs and the Class to safeguard their Personal Information and to implement adequate data security measures;

o. Whether Defendants breached that duty;

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

q. Whether Defendants 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;

r. Whether such representations were false with regard to storing and safeguarding Class members' Personal Information; and

s. Whether such representations were material with regard to storing and safeguarding Class members' Personal Information.

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*.)

56. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 55 as though fully stated herein.

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

58. Google represented that it would not disclose Google+ users' Personal Information without consent and/or notice. Google further represented that it would utilize sufficient data security protocols and mechanisms to protect Google+ users' Personal Information.

59. Defendants failed to abide by these representations. Defendants did not prevent improper disclosure of Plaintiffs' and the Class's Personal Information.

60. Defendants stored the Personal Information of Plaintiffs and members of their respective Classes in Defendants' electronic and consumer information databases. Defendants falsely represented to Plaintiffs and members of the Classes that the Personal Information databases were secure and that class members' Personal Information would remain private. Defendants 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' Personal Information

secure and prevented the loss or misuse of Plaintiffs' and the other class members' Personal Information.

61. Even without these misrepresentations, Plaintiffs and Class members were entitled to assume, and did assume Defendants would take appropriate measures to keep their Personal Information safe. Defendants did not disclose at any time that Plaintiffs' Personal Information was accessible to third party application vendors because Defendants' data security measures were inadequate, and Defendants was the only one in possession of that material information, which they had a duty to disclose. Defendants violated the UCL by misrepresenting, both by affirmative conduct and by omission, the security of its many systems and services, and its ability to honor the disclosure authorizations established by Plaintiffs and Class members for their Personal Information.

62. Defendants 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 Defendants had complied with these legal requirements, Plaintiffs and the other Class members would not have suffered the damages described herein.

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

64. Plaintiffs and the Class members suffered injury in fact and lost money or property as the result of Defendants' unlawful business practices. In particular, Plaintiffs' and Class members' Personal Information 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.

65. As a result of Defendants' 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*.)

66. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 55 as though fully stated herein.

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

68. Defendants stored the Personal Information of Plaintiffs and members of their respective Classes in their electronic and consumer information databases. Defendants represented to Plaintiffs and members of the classes that its Personal Information databases were secure and that class members' Personal Information would remain private and be disclosed only with expressed authorization. Defendants engaged in unfair acts and business practices by representing that would require expressed consent and authorization prior to disclosure of Personal Information to third parties.

69. Even without these misrepresentations, Plaintiffs and Class members were entitled to, and did, assume Defendants would take appropriate measures to keep their Personal Information safe. Defendants did not disclose at any time that Plaintiffs' Personal Information was vulnerable to unauthorized disclosure because Defendants' data security measures were inadequate, and Defendants were in sole possession of that material information, which they had a duty to disclose.

70. Defendants knew or should have known it did not employ reasonable measures that would have kept Plaintiffs' and the other Class members' Personal Information secure from unauthorized disclosure.

71. Defendants engaged in unfair acts and business practices by representing that they would not disclose this Personal Information without authorization, and/or by obtaining that Personal Information without authorization. Defendants also violated its commitment to maintain the confidentiality and security of the Personal Information 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.

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

73. **Defendant engaged in unfair business practices under the "tethering test."** Defendants' actions and omissions, as described in detail above, violated fundamental public policies expressed by the California Legislature. *See, e.g.,* Cal. Civ. Code § 1798.1 ("The Legislature declares that ... all individuals have a right of privacy in information pertaining to them.... The increasing use of computers ... has greatly magnified the potential risk to individual privacy that can occur from the maintenance of Personal Information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that Personal Information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern.") Defendants' acts and omissions, and the injuries caused by

them are thus "comparable to or the same as a violation of the law …" *Cel-Tech Communications, Inc. v. Los Angeles Cellular Telephone Co.* (1999) 20 Cal.4th 163, 187.

74. **Defendant engaged in unfair business practices under the "FTC test."** The harm caused by Defendants' actions and omissions, as described in detail above, is substantial in that it affects approximately 53 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' Personal Information to third parties without their consent, diminution in value of their Personal Information, 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' Personal Information remains in Defendants' possession, without adequate protection, and is also in the hands of those who obtained it without their consent. Defendants' actions and omissions violated, *inter alia*, Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45. *See, e.g., F.T.C. v. Wyndham Worldwide Corp.,* 10 F. Supp. 3d 602, 613 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015); *In re LabMD, Inc.*, FTC Docket No. 9357, FTC File No. 102-3099 (July 28, 2016) (failure to employ reasonable and appropriate measures to secure Personal Information collected violated § 5(a) of FTC Act); *In re BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148, FTC File No. 042-3160 (Sept. 20, 2005) (same); *In re CardSystems Solutions, Inc.*, FTC Docket No. C-4168, FTC File No. 052-3148 (Sept. 5, 2006) (same); *see also United States v. ChoicePoint, Inc.*, Civil Action No. 1:06-cv-0198-JTC (N.D. Ga. Oct. 14, 2009) ("failure to establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security. confidentiality, and integrity of Personal Information collected from or about consumers" violates § 5(a) of FTC Act); 15 U.S.C. § 45(n) (defining

"unfair acts or practices" as those that "cause[] or [are] likely to cause substantial injury to consumers which [are] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.").

75. Plaintiffs and the Class members suffered injury in fact and lost money or property as the result of Defendants' unfair business practices. In addition, their Personal Information 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.

76. As a result of Defendants' 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
Negligence

77. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 55 as though fully stated herein.

78. Defendants owed a duty to Plaintiffs and the Class to exercise reasonable care in safeguarding and protecting their Personal Information and keeping it from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties.

79. Defendants knew that the Personal Information of Plaintiffs and the Class was personal and sensitive information that is valuable to identity thieves and other criminals. Defendants also knew of the serious harms that could happen if the Personal Information 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 Personal Information, Defendants had a special relationship with Plaintiffs and the Class. Plaintiffs and the Class signed up for Defendants' services and agreed to provide their Personal

Information with the understanding that Defendants would take appropriate measures to protect it, and would inform Plaintiffs and the Class of any breaches or other security concerns that might call for action by Plaintiffs and the Class. But, Defendants did not. Defendants not only knew their data security was inadequate, Defendants also knew they did not have the tools to detect and document intrusions or exfiltration of Personal Information.

81. Defendants breached their duty to exercise reasonable care in safeguarding and protecting Plaintiffs' and the Class members' Personal Information by failing to adopt, implement, and maintain adequate security measures to safeguard that information and prevent unauthorized disclosure of Plaintiffs' and the other Class members' Personal Information.

82. Defendants also breached their duty to timely disclose that Plaintiffs' and the other class members' Personal Information had been, or was reasonably believed to have been, improperly obtained.

83. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and the Class, their Personal Information would not have been compromised, stolen, and viewed by unauthorized persons.

84. Defendants' negligence was a direct and legal cause of the theft of the Personal Information 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 Defendants' failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and the other class members' Personal Information. Defendants knew their systems and technologies for processing and securing the Personal Information of Plaintiffs and the Class had numerous security vulnerabilities.

86. As a result of this misconduct by Defendants, the Personal Information of Plaintiffs and the Class were compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their Personal Information was disclosed to third parties without their consent.

Fourth Claim for Relief
Invasion of Privacy

87. Plaintiffs repeats, realleges, and incorporates by reference the allegations contained in paragraphs 1 through 55 as through fully stated herein.

88. Google's terms and conditions designate California law as the sole applicable law governing the relationship between Google and its users.

89. The California Constitution expressly provides for a right to privacy. Cal. Const. Art. I, Sec. 1.

90. Google's terms of use for all times relevant to this matter provided that users' Personal Information would not be released to third parties without express consent.

91. Absent their express consent, Plaintiffs and the Class members used Google+ under the impression that Personal Information was safeguarded and would not be provided to or stolen by third parties.

92. Plaintiffs and the Class members had an interest in the protection and non-dissemination of the Personal Information that Defendants electronically stored, including the right not to have that Personal Information stolen and used for profit.

93. Absent the express consent of Google+ users, Defendants intentionally intruded on Plaintiffs' and the Class members' private life, seclusion, and solitude, protected under the California constitution as well as common law.

94. Defendants' wrongful conduct constitutes breach of the social norms underpinning the constitutionally-protected right to privacy.

95. Defendants' wrongful conduct harmed Plaintiffs and the Class members.

96. As a direct and proximate result of Defendants wrongful conduct, Plaintiffs and the Class members have suffered injury and are entitled to appropriate relief, including injunctive relief and damages.

Fifth Claim for Relief
Breach of Confidence

97. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 55 as though fully stated herein.

98. This claim is asserted against Defendants for breach of confidence concerning the Personal Information Plaintiffs and Class members provided to Defendants in confidence.

99. At all times during Plaintiffs' and Class members' interactions with Defendants, Defendants were fully aware of the confidential nature of the Personal Information that Plaintiffs and Class members shared with Defendants.

100. As alleged herein and above, Defendants' relationships with Plaintiffs and Class members were governed by the terms and expectations that Plaintiffs' and Class members' Personal Information would be collected, stored, and protected in confidence, and not disclosed to unauthorized third parties.

101. Plaintiffs and Class members provided their respective Personal Information to Defendants with the explicit and implicit understanding that Defendants would protect and not permit the Personal Information to be disseminated to any unauthorized third parties.

102. Defendant voluntarily received in confidence Plaintiffs' and Class members' Personal Information with the understanding that the Personal Information would not be disclosed or disseminated to the public or any unauthorized third parties.

103. Due to Defendants' failure to prevent, detect, and stop the 2018 Data Leaks from occurring, Plaintiffs' and Class members' Personal Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and all Class members' confidence and without their express permission.

104. As a direct and proximate cause of Defendants' actions and inactions, Plaintiffs and Class members have suffered damages.

105. But for Defendants' disclosure of Personal Information in violation of the parties' understanding of confidence, their Personal Information would not have been compromised, stolen, and viewed by unauthorized persons. Defendants' disclosure was a direct and legal cause of the theft of Plaintiffs' and Class members' Personal Information, as well as the resulting damages.

106. The injury and harm Plaintiffs and Class members suffered was the reasonably foreseeable result of Defendants' unauthorized disclosure of Plaintiffs' and Class members' Personal Information. Defendants knew its computer systems and technologies for accepting and securing Plaintiffs' and Class members' Personal Information had numerous security vulnerabilities, but Defendants continued to collect, store, and maintain Plaintiffs' and Class members' Personal Information, even after the First Data Leak.

107. As a result of Defendants' misconduct, Plaintiffs' and Class members' Personal Information was compromised, placing them at a greater risk of identity theft and subjecting them to identity theft and fraud, and their Personal Information was disclosed to unauthorized third parties without their consent. Plaintiffs and all Class members also suffered diminution in value of their Personal Information in that it is now easily available to hackers on the dark web. Plaintiffs and all Class members have also suffered consequential out of pocket losses for procuring credit freezes or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

ADDITIONAL CLAIMS ALLEGED ON BEHALF OF THE CALIFORNIA SUBCLASS ONLY

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

108. Plaintiff Matic repeats, realleges, and incorporates by reference the allegations contained in paragraphs 1 through 55 as though fully stated herein.

109. Plaintiff Matic brings this claim on behalf of the California Subclass.

110. 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).

111. 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).

112. Google is a business that owns, licenses, or maintains Personal Information about California residents. As alleged in detail above, Defendants 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 2018 Data Leaks.

113. As the direct and legal result of Defendants' violation of section 1798.81.5, Plaintiff Matic and the members of the California subclass were harmed because their Personal Information was compromised, placing them at a greater risk of identity theft and their Personal Information disclosed to third parties without their consent. Plaintiff Matic and

Class members also suffered diminution in value of their Personal Information in that it is now in the hands of unauthorized third parties who may use that information for their own personal and financial gain. The California subclass members are further damaged as their Personal Information remains Defendants' possession, without adequate protection, and is also in the hands of those who obtained it without their consent.

114. Plaintiff Matic 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.

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

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 Defendants' conduct was negligent, deceptive, unfair, and unlawful as alleged herein;

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

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

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

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

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

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

(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: December 11, 2018

/s/ *John A. Yanchunis*
JOHN A. YANCHUNIS

Attorney for Plaintiffs