

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

8 **MORGAN & MORGAN**  
**COMPLEX LITIGATION GROUP**  
 9 John A. Yanchunis (Pro Hac Vice Forthcoming)  
 10 *jyanchunis@ForThePeople.com*  
 Ryan J. McGee (Pro Hac Vice Forthcoming)  
 11 *rmcgee@ForThePeople.com*  
*Jonathan B. Cohen*  
 12 *jcohen@ForThePeople.com*  
 201 N. Franklin Street, 7th Floor  
 13 Tampa, Florida 33602  
 14 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

15 **UNITED STATES DISTRICT COURT**  
 16 **NORTHERN DISTRICT OF CALIFORNIA**

17  
 18 MATT MATIC, an individual and California  
 Resident, and ZAK HARRIS, an individual  
 19 and Florida Resident,

20 Plaintiffs,

21 v.

22 GOOGLE, LLC, and ALPHABET, INC.,

23 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**

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

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

**II. JURISDICTION AND VENUE.....2**

**III. PARTIES .....2**

    A. Plaintiffs .....2

    B. Defendants .....3

**IV. FACTUAL BACKGROUND.....3**

    A. Google’s Inadequate Data Security Allows the Massive Leak of Users’  
        Personal Information.....3

    B. Defendants Make A Business Decision Not To Disclose The First Data  
        Leak.....6

    C. Defendants Announce the Second Data Leak.....7

    D. Personal Information is Very Valuable on the Black Market.....8

**V. CLASS ACTION ALLEGATIONS .....10**

**VI. CLAIMS ALLEGED ON BEHALF OF ALL CLASSES.....16**

**First Claim for Relief.....16**

**Second Claim for Relief.....18**

**Third Claim for Relief .....21**

**Fourth Claim for Relief .....23**

**Fifth Claim for Relief.....24**

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

**Sixth Claim for Relief.....25**

**VIII. PRAYER FOR RELIEF.....28**

**IX. JURY TRIAL DEMANDED.....28**

1 For their Amended Class Action Complaint, Plaintiffs Matt Matic and Zak Harris, on  
2 behalf of themselves and all others similarly situated, allege the following against Defendant  
3 Google, LLC (“Google”) and Defendant Alphabet, Inc. (“Alphabet”), based on personal  
4 knowledge as to Plaintiffs and Plaintiffs’ own acts and on information and belief as to all  
5 other matters based upon, *inter alia*, the investigation conducted by and through Plaintiffs’  
6 undersigned counsel:

7 **SUMMARY OF THE CASE**

8 1. Launched in June 2011, Google+ (or Google Plus) is a social network owned  
9 and operated by Google for consumers with Google accounts. Google+ facilitates the sharing  
10 of information, photographs, weblinks, conversations, and other shared content similar in  
11 many respects to the Facebook news feed or Twitter stream.

12 2. Google+ was created as Google’s answer and rival to Facebook, but is widely  
13 seen as one of Google’s biggest failures.<sup>1</sup>

14 3. As part of the sign up process and as a consequence of interacting with the  
15 network, users of Google+ create, maintain, and update profiles containing significant  
16 amounts of Personal Information, including their names, birthdates, hometowns, addresses,  
17 locations, interests, relationships, email addresses, photos, and videos, amongst others,  
18 referred to herein as “Personal Information.”

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

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

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

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

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

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

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

10 **JURISDICTION AND VENUE**

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

16 10. Venue is proper under 28 U.S.C. § 1391(c) because Defendants are  
17 corporations that do business in and are subject to personal jurisdiction in this District. Venue  
18 is also proper because a substantial part of the events or omissions giving rise to the claims in  
19 this action occurred in or emanated from this District, including the decisions made by  
20 Defendants’ governance and management personnel that led to the data leak and the decision  
21 not to disclose the leak. Further, Google’s Terms of Service governing users in the United  
22 States provides for venue in the Northern District of California for all claims arising out of  
23 Plaintiffs’ relationship with Google.

24 **PARTIES**

25 **A. Plaintiffs**

26 11. Plaintiff Matt Matic is a resident and citizen of California. Plaintiff Matic  
27 opened a Google+ account and has used it for many years. Plaintiff Matic also uses a Gmail  
28

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

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

## 7 **B. Defendants**

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

10 14. Defendant Alphabet, Inc. (“Alphabet”), is a Delaware corporation with its  
11 principal headquarters in Mountain View, California. Alphabet is a public holding company  
12 formed in a corporate reorganization by Google. Through the corporate restructuring,  
13 Defendant Google is now a direct, wholly owned subsidiary of Defendant Alphabet.<sup>2</sup>

## 14 **FACTUAL BACKGROUND**

### 15 **A. Google’s Inadequate Data Security Allows the Massive Leak of Users’ Personal 16 Information**

17 15. Google’s Terms of Service make it clear that Google collects information  
18 from its users.<sup>3</sup> But at all relevant times, Google has maintained a Privacy Policy advising its  
19 users that: “When you use our services, you’re trusting us with your information. We  
20 understand this is a big responsibility and work hard to protect your information and put you  
21 in control.”<sup>4</sup> Further, Google represents that “We’ll share Personal Information outside of  
22 Google when we have your consent.”<sup>5</sup>

24  
25 <sup>2</sup> 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  
26 visited October 8, 2018).

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

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

<sup>5</sup> *Id.* (emphasis added).

1           16. Google represents to its users that:

- 2                   a. “You have choices regarding the information we collect and how it’s  
3                   used.”<sup>6</sup>
- 4                   b. “We’ll ask for your consent before using your information for a  
5                   purpose that isn’t covered in this Privacy Policy.”<sup>7</sup>
- 6                   c. “We’ll ask for your explicit consent to share any sensitive Personal  
7                   Information.”<sup>8</sup>

8           17. And importantly for the Data Breaches, Google represents to its users they can  
9 “[c]ontrol whom you share information with through your account on Google+.”<sup>9</sup>

10           18. Despite these representations, Google’s lax approach to data security resulted  
11 in the Data Leaks affecting approximately 53 million Google+ users over a period of at least  
12 3 years (the “2018 Data Leaks”).

13           19. On October 8, 2018, Alphabet announced that it would be permanently  
14 shutting down the consumer functionality of Google+.<sup>10</sup> Along with this announcement,  
15 Alphabet disclosed that a “software glitch” had allowed outside application (also “app”)  
16 vendors access to private Google+ profile data between 2015 and March 2018.

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

21  
22  
23  
24  
25  
26 \_\_\_\_\_  
<sup>6</sup> *Id.*

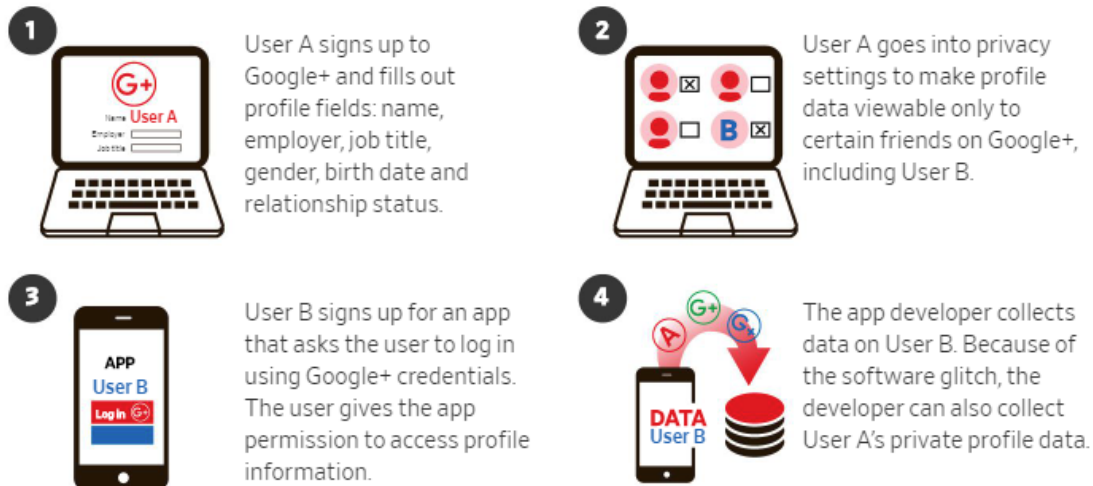
<sup>7</sup> *Id.*

<sup>8</sup> *Id.* (emphasis added).

<sup>9</sup> *Id.*

<sup>10</sup> THE WALL STREET JOURNAL, *Google Exposed User Data, Feared Repercussions of Disclosing to Public*,  
supra fn. 1.

1           21. The access allowed through this “glitch” is shown in the following  
2 illustration<sup>11</sup>:



12           22. Immediately, the First Data Leak drew comparisons to Facebook’s leak of  
13 user information to Cambridge Analytica and other third party app developers.<sup>12</sup>

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

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

23           25. Defendants advised that at least 438 third party applications may have used  
24 the API related to the First Data Leak and been allowed unauthorized access to Google+  
25 users’ data for nearly 3 years.<sup>13</sup>

26 \_\_\_\_\_  
27 <sup>11</sup> *Id.*

28 <sup>12</sup> *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](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).

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

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

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

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

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

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

21           31.     It has been reported that, faced with the news of this massive First Data Leak,  
22 Defendants made a calculated business decision, with the knowledge of Chief Executive  
23

---

24 <sup>13</sup> ZD Net, *Google Shuts Down Google+ After API Bug Exposed Details For Over 500,000 Users* (October 8,  
25 2018), <https://www.zdnet.com/article/google-shuts-down-google-after-api-bug-exposed-details-for-over-500000-users/> (last visited October 8, 2018).

26 <sup>14</sup> *Id.*

27 <sup>15</sup> Statt and Brandom, *Google will shut down Google+ four months early after second data leak* (Dec. 10,  
28 2018) <https://www.theverge.com/platform/amp/2018/12/10/18134541/google-plus-privacy-api-data-leak-developers>

<sup>16</sup> *Id.*

<sup>17</sup> THE WALL STREET JOURNAL, *Google Exposed User Data, Feared Repercussions of Disclosing to Public*, *supra* fn. 1.



1 Sundar Pichai, that disclosure of the First Data Leak might invite “regulatory interest” similar  
2 to what Facebook faced in the wake of the Cambridge Analytica debacle.<sup>18</sup>

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

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

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

### 12 **C. Defendants Announce the Second Data Leak**

13 35. In the wake of the increased attention from the First Data Leak in October  
14 2018, Defendants still operated the Google+ service, continuing to collect users’ Personal  
15 Information, with plans to shut the Google+ service down in August 2019.

16 36. Approximately one month following the First Data Leak, Defendants  
17 permitted the Second Data Leak to persist from November 7, 2018, through November 13,  
18 2018, when Defendants allegedly identified and fixed vulnerabilities that again permitted  
19 unauthorized third parties to access and aggregate users’ Personal Information.<sup>19</sup>

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

23 38. The Second Data Leak involved names, email addresses, occupations, ages,  
24 and other Personal Information, and was exposed to unauthorized third parties, despite users  
25 setting their accounts to private and explicitly denying Defendants the permission to share  
26 that Personal Information with unauthorized third parties.<sup>20</sup>

---

27 <sup>18</sup> *Id.*

28 <sup>19</sup> Statton and Brandom, *supra*, n.16

<sup>20</sup> Statton and Brandom, *supra* n.16

1 **D. Personal Information is Very Valuable on the Black Market**

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

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

11 In addition to the losses that result when identity thieves fraudulently open  
12 accounts or misuse existing accounts, . . . individual victims often suffer  
13 indirect financial costs, including the costs incurred in both civil litigation  
14 initiated by creditors and in overcoming the many obstacles they face in  
15 obtaining or retaining credit. Victims of non-financial identity theft, for  
16 example, health-related or criminal record fraud, face other types of harm  
17 and frustration.

18 In addition to out-of-pocket expenses that can reach thousands of dollars  
19 for the victims of new account identity theft, and the emotional toll  
20 identity theft can take, some victims have to spend what can be a  
21 considerable amount of time to repair the damage caused by the identity  
22 thieves. Victims of new account identity theft, for example, must correct  
23 fraudulent information in their credit reports and monitor their reports for  
24 future inaccuracies, close existing bank accounts and open new ones, and  
25 dispute charges with individual creditors.<sup>21</sup>

26 41. To put it into context, as demonstrated in the chart below, the 2013 Norton  
27 Report, based on one of the largest consumer cybercrime studies ever conducted, estimated  
28 that the global price tag of cybercrime was around \$113 billion at that time, with the average  
cost per victim being \$298 dollars.

---

<sup>21</sup> 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>.



10 42. The problems associated with identity theft are exacerbated by the fact that

11 many identity thieves will wait years before attempting to use the Personal Information they

12 have obtained. Indeed, in order to protect themselves, Class members will need to remain

13 vigilant against unauthorized data use for years and decades to come.

14 43. Once stolen, Personal Information can be used in a number of different ways.

15 One of the most common is that it is offered for sale on the “dark web,” a heavily encrypted

16 part of the Internet that makes it difficult for authorities to detect the location or owners of a

17 website. The dark web is not indexed by normal search engines such as Google and is only

18 accessible using a Tor browser (or similar tool), which aims to conceal users’ identities and

19 online activity. The dark web is notorious for hosting marketplaces selling illegal items such

20 as weapons, drugs, and Personal Information.<sup>22</sup> Websites appear and disappear quickly,

21 making it a very dynamic environment.

22

23 44. Once someone buys Personal Information, it is then used to gain access to

24 different areas of the victim’s digital life, including bank accounts, social media, and credit

25

26

27

28 <sup>22</sup> Brian Hamrick, [The dark web: A trip into the underbelly of the internet](http://www.wlwt.com/article/the-dark-web-a-trip-into-the-underbelly-of-the-internet/8698419), 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>.

1 card details. During that process, other sensitive data may be harvested from the victim's  
2 accounts, as well as from those belonging to family, friends, and colleagues.

3 **CLASS ACTION ALLEGATIONS**

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

7 **A. The United States Class**

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

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

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

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

22 48. **Numerosity:** The members of each Class are so numerous that joinder of all  
23 members of any Class would be impracticable. Defendants have indicated that at least  
24 500,000 people had their Google+ accounts compromised as a result of the First Data Leak,  
25 and as many as 52,500,000 people had their Google+ accounts compromised as a result of  
26 the Second Data Leak. The identity of these Google+ users can be determined through  
27 records and documents maintained by Defendants.  
28

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

- 4           i.    Whether Defendants represented to the Class that it would safeguard  
5           Class members' Personal Information;
- 6           ii.   Whether Defendants owed a legal duty to Plaintiffs and the Class to  
7           exercise due care in collecting, storing, and safeguarding their Personal  
8           Information;
- 9           iii.   Whether Defendants breached a legal duty to Plaintiffs and the Class to  
10           exercise due care in collecting, storing, and safeguarding their Personal  
11           Information;
- 12           iv.   Whether third parties improperly obtained Plaintiffs' and Class members'  
13           Personal Information without authorization or in excess of any  
14           authorization;
- 15           v.    Whether Defendants were aware of other third parties' collection of  
16           Plaintiffs' and Class members' Personal Information without  
17           authorization or in excess of any authorization;
- 18           vi.   Whether Defendants knew about the First Data Leak before it was  
19           announced to the public and Defendants failed to timely notify the public  
20           of the First Data Leak;
- 21           vii.   Whether Defendants knew about the Second Data Leak before it was  
22           announced to the public and Defendants failed to timely notify the public  
23           of the Second Data Leak;
- 24           viii.   Whether Defendants' conduct violated Cal. Civ. Code § 1750, *et seq.*;
- 25           ix.   Whether Defendants' conduct was an unlawful or unfair business practice  
26           under Cal. Bus. & Prof. Code § 17200, *et seq.*;
- 27
- 28

- 1           x. Whether Defendants' conduct violated the Consumer Records Act, Cal.
- 2           Civ. Code § 1798.80 *et seq.*;
- 3           xi. Whether Defendants' conduct violated § 5 of the Federal Trade
- 4           Commission Act, 15 U.S.C. § 45, *et seq.*,
- 5           xii. Whether Plaintiffs and the Class are entitled to equitable relief, including,
- 6           but not limited to, injunctive relief and restitution; and
- 7           xiii. Whether Plaintiffs and the other Class members are entitled to actual,
- 8           statutory, or other forms of damages, and other monetary relief.

9           50. Defendants engaged in a common course of conduct giving rise to the legal  
10 rights sought to be enforced by Plaintiffs individually and on behalf of the members of the  
11 class. Similar or identical statutory and common law violations, business practices, and  
12 injuries are involved. Individual questions, if any, pale by comparison, in both quantity and  
13 quality, to the numerous common questions that dominate this action.

14  
15           51. **Typicality:** Plaintiffs' claims are typical of the claims of the other members of  
16 their respective classes because, among other things, Plaintiffs and the other Class members  
17 were injured through the substantially uniform misconduct by Defendants. Plaintiffs are  
18 advancing the same claims and legal theories on behalf of themselves and all other Class  
19 members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and  
20 those of other Class members arise from the same operative facts and are based on the same  
21 legal theories.

22  
23           52. **Adequacy of Representation:** Plaintiffs are adequate representatives of the  
24 classes because their interests do not conflict with the interests of the other Class members  
25 they seek to represent; they have retained counsel competent and experienced in complex  
26 class action litigation and Plaintiffs will prosecute this action vigorously. The Class  
27 members' interests will be fairly and adequately protected by Plaintiffs and their counsel.

1           53.     **Superiority:** A class action is superior to any other available means for the  
2 fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be  
3 encountered in the management of this matter as a class action. The damages, harm, or other  
4 financial detriment suffered individually by Plaintiffs and the other members of their  
5 respective classes are relatively small compared to the burden and expense that would be  
6 required to litigate their claims on an individual basis against Defendants, making it  
7 impracticable for Class members to individually seek redress for Defendants' wrongful  
8 conduct. Even if Class members could afford individual litigation, the court system could  
9 not. Individualized litigation would create a potential for inconsistent or contradictory  
10 judgments, and increase the delay and expense to all parties and the court system. By  
11 contrast, the class action device presents far fewer management difficulties and provides the  
12 benefits of single adjudication, economies of scale, and comprehensive supervision by a  
13 single court.  
14

15           54.     Further, Defendants has acted or refused to act on grounds generally  
16 applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief  
17 with regard to the members of the Class as a whole is appropriate under Rule 23(b)(2) of the  
18 Federal Rules of Civil Procedure.  
19

20           55.     Likewise, particular issues under Rule 23(c)(4) are appropriate for  
21 certification because such claims present only particular, common issues, the resolution of  
22 which would advance the disposition of this matter and the parties' interests therein. Such  
23 particular issues include, but are not limited to:  
24

- 25           a.     Whether Class members' Personal Information was improperly obtained by  
26                 third parties;  
27  
28

- 1           b.     Whether (and when) Defendants knew about any security vulnerabilities that  
2           led to the First Data Leak before they were announced to the public and  
3           whether Defendants failed to timely notify the public of those vulnerabilities  
4           and the First Data Leak;
- 5           c.     Whether (and when) Defendants knew about any security vulnerabilities that  
6           led to the Second Data Leak before they were announced to the public and  
7           whether Defendants failed to timely notify the public of those vulnerabilities  
8           and the Second Data Leak;
- 9           d.     Whether Defendants’ conduct was an unlawful or unfair business practice  
10          under Cal. Bus. & Prof. Code § 17200, *et seq.*;
- 11          e.     Whether Defendants’ representations that it would secure and protect the  
12          Personal Information of Plaintiffs and members of the classes were facts that  
13          reasonable persons could be expected to rely upon when deciding whether to  
14          use Defendants’ services;
- 15          f.     Whether Defendants misrepresented the safety of its many systems and  
16          services, specifically the security thereof, and its ability to safely store  
17          Plaintiffs’ and Class members’ Personal Information;
- 18          g.     Whether Defendants concealed crucial information about their inadequate data  
19          security measures from Plaintiffs and the Class;
- 20          h.     Whether Defendants failed to comply with their own policies and applicable  
21          laws, regulations, and industry standards relating to data security;
- 22          i.     Whether Defendants knew or should have known that they did not employ  
23          reasonable measures to keep Plaintiffs’ and Class members’ Personal  
24          Information secure and protected;
- 25          j.     Whether Defendants failed to implement reasonable measures to keep Plaintiffs’ and Class members’ Personal  
26          Information secure and protected;
- 27          k.     Whether Defendants failed to implement reasonable measures to keep Plaintiffs’ and Class members’ Personal  
28          Information secure and protected;



1 Information secure and prevent the unauthorized disclosure of that  
2 information;

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

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

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

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

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

15 o. Whether Defendants breached that duty;

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

19 q. Whether Defendants negligently and materially failed to adhere to its posted  
20 privacy policy with respect to the extent of its disclosure of users’ data, in  
21 violation of California Business and Professions Code § 22576;

22 r. Whether such representations were false with regard to storing and  
23 safeguarding Class members’ Personal Information; and  
24  
25  
26  
27  
28

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

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

4 **First Claim for Relief**

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

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

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

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

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

18 60. Defendants stored the Personal Information of Plaintiffs and members of their  
19 respective Classes in Defendants' electronic and consumer information databases.  
20 Defendants falsely represented to Plaintiffs and members of the Classes that the Personal  
21 Information databases were secure and that class members' Personal Information would  
22 remain private. Defendants knew or should have known it did not employ reasonable,  
23 industry standard, and appropriate security measures that complied "with federal regulations"  
24 and that would have kept Plaintiffs' and the other Class members' Personal Information  
25  
26  
27  
28

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

3 61. Even without these misrepresentations, Plaintiffs and Class members were  
4 entitled to assume, and did assume Defendants would take appropriate measures to keep their  
5 Personal Information safe. Defendants did not disclose at any time that Plaintiffs' Personal  
6 Information was accessible to third party application vendors because Defendants' data  
7 security measures were inadequate, and Defendants was the only one in possession of that  
8 material information, which they had a duty to disclose. Defendants violated the UCL by  
9 misrepresenting, both by affirmative conduct and by omission, the security of its many  
10 systems and services, and its ability to honor the disclosure authorizations established by  
11 Plaintiffs and Class members for their Personal Information.  
12

13 62. Defendants also violated the UCL by failing to implement reasonable and  
14 appropriate security measures or follow industry standards for data security, and failing to  
15 comply with its own posted privacy policies. If Defendants had complied with these legal  
16 requirements, Plaintiffs and the other Class members would not have suffered the damages  
17 described herein.  
18

19 63. Defendants' acts, omissions, and misrepresentations as alleged herein were  
20 unlawful and in violation of, *inter alia*, Cal. Civ. Code § 1798.81.5(b), Section 5(a) of the  
21 Federal Trade Commission Act, 15 U.S.C. § 45(a), Cal. Bus. & Prof. Code § 22576 (as a  
22 result of Google failing to comply with its own posted privacy policies).  
23

24 64. Plaintiffs and the Class members suffered injury in fact and lost money or  
25 property as the result of Defendants' unlawful business practices. In particular, Plaintiffs' and  
26 Class members' Personal Information was taken and is in the hands of those who will use it  
27  
28

1 for their own advantage, or is being sold for value, making it clear that information is of  
2 tangible value.

3 65. As a result of Defendants' unlawful business practices, violations of the UCL,  
4 Plaintiffs and the Class members are entitled to restitution, disgorgement of wrongfully  
5 obtained profits and injunctive relief.

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

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

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

13 68. Defendants stored the Personal Information of Plaintiffs and members of their  
14 respective Classes in their electronic and consumer information databases. Defendants  
15 represented to Plaintiffs and members of the classes that its Personal Information databases  
16 were secure and that class members' Personal Information would remain private and be  
17 disclosed only with expressed authorization. Defendants engaged in unfair acts and business  
18 practices by representing that would require expressed consent and authorization prior to  
19 disclosure of Personal Information to third parties.  
20

21 69. Even without these misrepresentations, Plaintiffs and Class members were  
22 entitled to, and did, assume Defendants would take appropriate measures to keep their  
23 Personal Information safe. Defendants did not disclose at any time that Plaintiffs' Personal  
24 Information was vulnerable to unauthorized disclosure because Defendants' data security  
25 measures were inadequate, and Defendants were in sole possession of that material  
26 information, which they had a duty to disclose.  
27  
28

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

4           71. Defendants engaged in unfair acts and business practices by representing that  
5 they would not disclose this Personal Information without authorization, and/or by obtaining  
6 that Personal Information without authorization. Defendants also violated its commitment to  
7 maintain the confidentiality and security of the Personal Information of Plaintiffs and their  
8 respective Classes, and failed to comply with its own policies and applicable laws,  
9 regulations, and industry standards relating to data security.

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

15           73. **Defendant engaged in unfair business practices under the “tethering**  
16 **test.”** Defendants' actions and omissions, as described in detail above, violated fundamental  
17 public policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1  
18 (“The Legislature declares that ... all individuals have a right of privacy in information  
19 pertaining to them.... The increasing use of computers ... has greatly magnified the potential  
20 risk to individual privacy that can occur from the maintenance of Personal Information.”);  
21 Cal. Civ. Code § 1798.81.5(a) (“It is the intent of the Legislature to ensure that Personal  
22 Information about California residents is protected.”); Cal. Bus. & Prof. Code § 22578 (“It is  
23 the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is  
24 a matter of statewide concern.”) Defendants' acts and omissions, and the injuries caused by  
25  
26  
27  
28

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

3 **74. Defendant engaged in unfair business practices under the “FTC test.”**

4 The harm caused by Defendants’ actions and omissions, as described in detail above, is  
5 substantial in that it affects approximately 53 million Class members and has caused those  
6 persons to suffer actual harms. Such harms include a substantial risk of identity theft,  
7 disclosure of Class members’ Personal Information to third parties without their consent,  
8 diminution in value of their Personal Information, consequential out of pocket losses for  
9 procuring credit freeze or protection services, identity theft monitoring, and other expenses  
10 relating to identity theft losses or protective measures. This harm continues given the fact  
11 that Class members’ Personal Information remains in Defendants’ possession, without  
12 adequate protection, and is also in the hands of those who obtained it without their consent.  
13 Defendants’ actions and omissions violated, *inter alia*, Section 5(a) of the Federal Trade  
14 Commission Act, 15 U.S.C. § 45. *See, e.g., F.T.C. v. Wyndham Worldwide Corp.*, 10 F.  
15 Supp. 3d 602, 613 (D.N.J. 2014), *aff’d*, 799 F.3d 236 (3d Cir. 2015); *In re LabMD, Inc.*, FTC  
16 Docket No. 9357, FTC File No. 102-3099 (July 28, 2016) (failure to employ reasonable and  
17 appropriate measures to secure Personal Information collected violated § 5(a) of FTC Act);  
18 *In re BJ’s Wholesale Club, Inc.*, FTC Docket No. C-4148, FTC File No. 042-3160 (Sept. 20,  
19 2005) (same); *In re CardSystems Solutions, Inc.*, FTC Docket No. C-4168, FTC File No.  
20 052-3148 (Sept. 5, 2006) (same); *see also United States v. ChoicePoint, Inc.*, Civil Action  
21 No. 1:06-cv-0198-JTC (N.D. Ga. Oct. 14, 2009) (“failure to establish and implement, and  
22 thereafter maintain, a comprehensive information security program that is reasonably  
23 designed to protect the security, confidentiality, and integrity of Personal Information  
24 collected from or about consumers” violates § 5(a) of FTC Act); 15 U.S.C. § 45(n) (defining  
25  
26  
27  
28

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

4 75. Plaintiffs and the Class members suffered injury in fact and lost money or  
5 property as the result of Defendants’ unfair business practices. In addition, their Personal  
6 Information was taken and is in the hands of those who will use it for their own advantage, or  
7 is being sold for value, making it clear that the hacked information is of tangible value.

8 76. As a result of Defendants’ unfair business practices, violations of the UCL,  
9 Plaintiffs and the Class members are entitled to restitution, disgorgement of wrongfully  
10 obtained profits, and injunctive relief.

11  
12 **Third Claim for Relief**  
13 **Negligence**

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

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

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

24 80. By being entrusted by Plaintiffs and the Class to safeguard their Personal  
25 Information, Defendants had a special relationship with Plaintiffs and the Class. Plaintiffs  
26 and the Class signed up for Defendants’ services and agreed to provide their Personal  
27  
28

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

6 81. Defendants breached their duty to exercise reasonable care in safeguarding  
7 and protecting Plaintiffs' and the Class members' Personal Information by failing to adopt,  
8 implement, and maintain adequate security measures to safeguard that information and  
9 prevent unauthorized disclosure of Plaintiffs' and the other Class members' Personal  
10 Information.  
11

12 82. Defendants also breached their duty to timely disclose that Plaintiffs' and the  
13 other class members' Personal Information had been, or was reasonably believed to have  
14 been, improperly obtained.  
15

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

19 84. Defendants' negligence was a direct and legal cause of the theft of the  
20 Personal Information of Plaintiffs and the Class and all resulting damages.

21 85. The injury and harm suffered by Plaintiffs and the Class members was the  
22 reasonably foreseeable result of Defendants' failure to exercise reasonable care in  
23 safeguarding and protecting Plaintiffs' and the other class members' Personal Information.  
24 Defendants knew their systems and technologies for processing and securing the Personal  
25 Information of Plaintiffs and the Class had numerous security vulnerabilities.  
26  
27  
28









1 110. California Civil Code section 1798.80, *et seq.*, known as the “Customer  
2 Records Act” (“CRA”) was enacted to “encourage business that own, license, or maintain  
3 Personal Information about Californians to provide reasonable security for that information.”  
4 Cal. Civ. Code § 1798.81.5(a)(1).

5 111. Section 1798.81.5, subdivision (b) of the CRA requires any business that  
6 “owns, licenses, or maintains Personal Information about a California resident” to  
7 “implement and maintain reasonable security procedures and practices appropriate to the  
8 nature of the information,” and “to protect the Personal Information from unauthorized  
9 access, destruction, use, modification, or disclosure.” Section 1798.81.5, subdivision  
10 (d)(1)(B) defines “Personal Information” as including “A username or email address in  
11 combination with a password or security question and answer that would permit access to an  
12 online account.” “Personal Information” also includes an individual’s first name or first  
13 initial in combination with a social security number, driver’s license number, account number  
14 or credit or debit card number and access code, medical information, or health insurance  
15 information. Cal. Civ. Code § 1798.82(h).  
16  
17

18 112. Google is a business that owns, licenses, or maintains Personal Information  
19 about California residents. As alleged in detail above, Defendants failed to implement and  
20 maintain reasonable security procedures and practices appropriate to the nature of the  
21 information, and protect the Personal Information from unauthorized access, destruction, use,  
22 modification, or disclosure, resulting in the 2018 Data Leaks.  
23

24 113. As the direct and legal result of Defendants’ violation of section 1798.81.5,  
25 Plaintiff Matic and the members of the California subclass were harmed because their  
26 Personal Information was compromised, placing them at a greater risk of identity theft and  
27 their Personal Information disclosed to third parties without their consent. Plaintiff Matic and  
28

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

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

9 115. Defendants' misconduct as alleged herein is fraud under Civil Code §  
10 3294(c)(3) in that it was deceit or concealment of a material fact known to the Defendants  
11 conducted with the intent on the part of Defendants of depriving Plaintiffs and the Class of  
12 "legal rights or otherwise causing injury." In addition, Defendants' misconduct as alleged  
13 herein is malice or oppression under Civil Code § 3294(c)(1) and (2) in that it was despicable  
14 conduct carried on by Defendants with a willful and conscious disregard of the rights or  
15 safety of Plaintiffs and the Class and despicable conduct that has subjected Plaintiffs and the  
16 Class to cruel and unjust hardship in conscious disregard of their rights. As a result, Plaintiffs  
17 and the Class are entitled to punitive damages against Defendants under Civil Code §  
18 3294(a).  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**PRAYER FOR RELIEF**

1  
2 WHEREFORE, Plaintiffs, individually and on behalf of the other Class members,  
3 respectfully request that this Court enter an Order:

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

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

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

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

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

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

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

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

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

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

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

23  
24  
25  
26 **JURY TRIAL DEMANDED**

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

3 Dated: December 11, 2018

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

*Attorney for Plaintiffs*

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