LAW OFFICES OF RONALD A. MARRON
RONALD A. MARRON (SBN 175650)
ron@consumersadvocates.com
ALEXIS M. WOOD (SBN 270200)
alexis@consumersadvocates.com
KAS L. GALLUCCI (SBN 288709)
kas@consumersadvocates.com
651 Arroyo Drive
San Diego, California 92103
Telephone: (619) 696-9006
Facsimile: (619) 564-6665

Attorneys for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

JENNIFER CHEN, individually and on behalf of all others similarly situated,

Plaintiff,

v.

FLO HEALTH, INC.

Defendant.

Case No.:

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff JENNIFER CHEN, on behalf of herself and all others similarly situated ("Plaintiff"), by and through her undersigned counsel, hereby sues Defendant Flo Heath, Inc. ("Defendant" or "Flo") and, upon information and belief and investigation of counsel, alleges as follows:

I. INTRODUCTION

1. This is an action brought by Plaintiff after knowledge that her personal identifying information has been tracked, collected, and shared by Defendant to dozens of third parties, including Google, LLC ("Google"); Google's separate marketing service, Fabric ("Fabric"); Facebook, Inc., through its Facebook Analytics tool ("Facebook"); marketing firm AppsFlyer, Inc. ("AppsFlyer") and analytics firm Flurry, Inc. ("Flurry") for targeted advertising and other commercial exploitation, in direct violation of California state laws and without limiting what these companies could do with the users' information. This personal information was provided to these third parties despite Defendant promising users that it would keep their health data private. The collection and sharing of Plaintiff's private health data presents an egregious invasion of Plaintiff's privacy. Furthermore, the transfer of data by Defendant to third parties harmed Plaintiff by, among other things, diminishing the value of Plaintiff's personal information and the privacy violation caused when the extracted data is used to target and profile Plaintiff with unwanted and/or harmful content.

2. The gravity of these data privacy violations cannot be overstated. In fact, a growing and insidious practice is to collect unique data from consumers to build a profile which is used to allow third parties and data brokers to follow users' activities across their devices with essentially no limit. This practice is unique and more damaging than the practice of tracking consumers' browsing activity with cookies.

3. Defendant had the affirmative duty to safeguard consumers' device information and private health information and, at the very minimum, to disclose the

access, collection, and dissemination of consumers' data. Defendant failed to fulfill such duties and in fact misrepresented that the data would be safeguarded.

4. Plaintiff seeks an injunction to stop Defendant's unlawful practices and sequester its unlawfully obtained information, an award of reasonable damages for the violations, and attorneys' fees and costs.

II. JURISDICTION AND VENUE

5. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d), because at least one member of the Class, as defined below is a citizen of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interest and costs.

6. The Court has personal jurisdiction over Defendant because Defendant has a principal place of business at 541 Jefferson Ave Ste 100, Redwood City, CA 94063 and regularly conducts business in California.

7. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because the injury in this case substantially occurred in this District.

III. PARTIES

8. Plaintiff Jennifer Chen ("Plaintiff") is a resident of Roseville, California.

9. Defendant Flo is a Delaware corporation with its registered address at 1013 Centre Road, Suite 4030B, Wilmington, Delaware 19805. Defendant also maintains a principal place of business in California at 541 Jefferson Ave Ste 100, Redwood City, CA 94063. Defendant is registered in California as C4312974.

10. Defendant has developed, advertised, offered for sale, sold, and distributed, the Flo Period & Ovulation Tracker, a mobile application ("app") powered by artificial intelligence that functions as an ovulation calendar, period tracker, and pregnancy guide ("Flo App").

IV. FACTUAL ALLEGATIONS

11. Millions of women use the Flo App, giving Defendant private details of their menstruation and gynecological health in hopes it will aid in ovulation and aid in pregnancy and childbirth.

12. The Flo App is available for download for free in online stores, including Google's "Play Store" and Apple's "App Store." Flo App users also have the option of purchasing subscription plans for a monthly fee.

13. The Flo App is one of the most popular health and fitness apps available to consumers. Since 2016 more than 150 million users have downloaded the Flo App, including more than 16 million users across the United States and more than 19 million users in the European Union ("EU") and Switzerland. In 2019, the Flo App was the most downloaded health and fitness app in the Apple App store and was the "App of the Day" in the Apple Store in over 30 counties. *See* https://flo.health/flo-health-inc/news/most-installed-app (last visited February 2, 2021).

14. Most adult consumers are unaware that the apps they download are specifically engineered to collect personal information surreptitiously and unlawfully from their mobile device, and then "share" that information for profit to advertisers.

15. App developers contract, for profit, with third parties for the right to embed third-party computer code into the developers' apps, for various purposes.

16. Advertising-specific SDKs (Software Development Kits) are blocks of computer code which operate to secretly collect an app user's personal information and track online behavior to facilitate behavioral advertising or marketing analysis.

17. In the case of an advertising SDK, the creator of the SDK will embed its SDK code into the underlying code of the app itself, collect personal information to serve behavioral advertisements, and then pay the app developer based on the number of ads shown.

18. This practice is a substantial source of many app developers' revenue, enabling app developers to allow users to download the apps without charging a purchase price. This is a common practice as demonstrated in 2020 with 96.1% of Android apps on the Google Play Store being free to download.[1]

19. Unbeknownst to users of the Flo App, in partnership with the SDKs, Defendant collects personal health data and tracks online behavior to profile users for targeted advertising.

20. As soon as a user downloads and opens up the Flo App his or her mobile device, Defendant immediately begins to collect personal information, currently defined in Defendant's Privacy Policy as name, email address, gender, date of birth, password or passcode, place of residence and associated location information, ID, weight, body temperature, menstrual cycle dates, various symptoms related to the user's menstrual cycle and health, and other private health information including sexual activities, well-being, and related activities, including personal life. *See* https://flo.health/privacy-policy#1 (last visited Feb. 26, 2021).

21. Targeted advertising is driven by users' personal data and employs sophisticated algorithms that interpret the personal data to determine the most effective advertising for individual users.

22. When a user is engaged in the Flo App every action on the device the user is using is linked to a unique and persistent identifier that constructs a profile of the user on that mobile device. These identifying numbers are unique to each device and put in place by app developers so that their SDK partners can collect the users' personal information and build an immense online profile across all the devices they use. Their app usage, geographic location (including likely domicile), and internet

[1] "Android and Google Play Statistics," AppBrain (October 15, 2020), *available at* https://www.appbrain.com/stats/free-and-paid-android-applications (last visited Feb. 26, 2021).

navigation all help to build a personal profile.

23. In sum, personal information is collected by Defendant and its SDK partners, which is then sold to third parties who track and use the collected information and analyze it with sophisticated algorithms to create a user profile. This profile is then used to serve behavioral advertising to individuals whose profile fits a set of demographic and behavioral traits.

What Are Persistent Identifiers

24. Defendant and its SDK partners track behavior while using the app by obtaining critical pieces of data from the mobile devices, including "persistent identifiers." These identifiers are a set of unique data points (typically numbers and letters), akin to a social security number, that can link one specific individual to all the apps on her device and her activity on those apps, allowing her to be tracked over time and across devices (*e.g.,* smart phones, tablets, laptops, desktops and smart TVs).

25. The common persistent identifiers for Apple are the ID for Advertisers ("IDFA") and ID for Vendors ("IDFV"). Both the IDFA and the IDFV are unique, alphanumeric strings that are used to identify an individual device—and the individual who uses that device—in order to track and profile the user, and to serve her with targeted advertising.

26. The common persistent identifiers in the Android operating system are the Android Advertising ID ("AAID") and the Android ID. The AAID and Android ID are unique, alphanumeric strings assigned to a user's device and used by apps and third parties to track and profile the user, and to serve her targeted advertising.

27. Additional persistent identifiers include data about a specific device, including details about its hardware—such as the device's brand (e.g., Apple or Android), the type of device (*e.g.*, iPhone, Galaxy, iPad)—and details about its software, such as its operation system (*e.g.*, iOS or Android). This data can also include more detailed information, such as the network carriers (*e.g.*, Sprint, T-

Mobile, AT&T), whether it is connected to Wi-Fi, and the "name" of the device. The name of the device is often particularly personal, as the default device name is frequently configured to include users' first and/or last names. In combination, the pieces of data provide a level of detail about the given device that allows that device and its user to be identified individually, uniquely, and persistently.

28. The Center for Digital Democracy, and the FTC described how and why a persistent identifier alone facilitates behavioral advertising:

> With the increasing use of new tracking and targeting techniques, any meaningful distinctions between personal and so-called non-personal information have disappeared. This is particularly the case with the proliferation of personal digital devices such as smart phones and Internet-enabled game consoles, which are increasingly associated with individual users, rather than families. This means that marketers do not need to know the name, address, or email of a user in order to identify, target and contact that particular user.

See Comments of The Center for Digital Democracy, et al., FTC, In the Matter of Children's Online Privacy Protection Rule at 13-14 (Dec. 23, 2011).[2]

29. A 2014 report by the Senate Committee on Homeland Security and Governmental Affairs entitled "Online Advertising and Hidden Hazards to Consumer Security and Data Privacy" amplifies this concern in light of the growth of third-party trackers that operate behind the scenes in routine online traffic:

> Although consumers are becoming increasingly vigilant about safeguarding the information they share on the Internet, many are less informed about the plethora of information created about them by online companies as they travel

[2] *See also* Jessica Rich, Director, FTC Bureau of Consumer Protection, Keeping Up with the Online Advertising Industry (Apr. 21, 2016), available at https://www.ftc.gov/news-events/blogs/business-blog/2016/04/keeping-online-advertising-industry (last visited Feb. 26, 2021).

> the Internet. A consumer may be aware, for example, that a search engine provider may use the search terms the consumer enters in order to select an advertisement targeted to his interests. Consumers are less aware, however, of the true scale of the data being collected about their online activity. A visit to an online news site may trigger interactions with hundreds of other parties that may be collecting information on the consumer as he travels the web. The Subcommittee found, for example, a trip to a popular tabloid news website triggered a user interaction with some 352 other web servers as well.…The sheer volume of such activity makes it difficult for even the most vigilant consumer to control the data being collected or protect against its malicious use. [3]

30. While disclosing a user's personal data to select and serve an advertisement (or to conduct any third-party analytics or otherwise monetize user data), Defendant and its partner SDKs pass identifying user data to an ever-increasing host of third parties, who, in turn, may pass along that same data to their affiliates. Each entity may use that data to track users over time and across the Internet, on a multitude of increasingly complex online pathways, with the shared goal of targeting users with advertisements.

31. The ability to serve targeted advertisements to (or to otherwise profile) a specific user no longer turns upon obtaining the kinds of data with which most consumers are familiar (name, email addresses, etc.), but instead on the surreptitious collection of persistent identifiers, which are used in conjunction with other data

---

[3] Staff Report, *Online Advertising and Hidden Hazards to Consumer Security and Data Privacy*, Permanent Subcommittee on Investigations of the U.S. Senate Homeland Security and Governmental Affairs Committee (May 15, 2014), at 1, available at https://www.hsgac.senate.gov/media/permanent-subcommittee-on-investigations-releases-report-online-advertising-and-hidden-hazards-to-consumer-security-and-data-privacy- (accessed February 26, 2021).

points to build robust online profiles. These persistent identifiers are better tracking tools than traditional identifiers because they are unique to each individual, making them more akin to a social security number. Once a persistent identifier is sent "into the marketplace," it is exposed to—and thereafter may be collected and used by—an almost innumerable set of third parties.

32. Data harvesting is the fastest growing industry in the entire country. Between 2016 and 2018, the value of information mined from Americans increased by 86% for Facebook and 40% for Google. Overall, the value internet companies derive from Americans' personal data increased almost 54%. Conservative estimates suggest that in 2018, internet companies earned $202 per American user. In 2022, that value is expected to be $200 billion industry wide, or $434 per user, also a conservative estimate. R Shapiro, What Your Data Is Really Worth to Facebook, Washington Monthly (July/Aug. 2019), available https://washingtonmonthly.com/magazine/july-august-2019/what-your-data-is-really-worth-to-facebook/ (last visited Feb. 26, 2021); *see also* R Shapiro & A Siddhartha, Who owns American's Personal Information and What is it Worth?, available at https://assets.futuremajority.org/uploads/report-for-future-majority-on-the-value-of-people-s-personal-data-shapiro-aneja-march-8-2019.pdf (last accessed Feb. 26, 2021).

Defendant's Disclosure of Private Health Information

33. Defendant tracks "Standard App Events," records of routine app functions (like opening or closing the app), as well as "Custom App Events." Custom App Events which are personal (such as when a user enters menstruation dates).

34. Despite representing that it would keep users' health data secret, Defendant disclosed health information of Flo App users to various third parties by integrating into the Flo App software SDK from the third-party marketing and analytics firms including, Facebook, Flurry, Fabric, AppsFlyer, and Google. These

SDKs gathered the unique advertising or device identifiers and Custom App Events of the millions of Flo App users.

35. On February 22, 2019, the *Wall Street Journal* reported that it was able to intercept unencrypted identifying health information transmitted by the Flo App to Facebook. The report found that this information included a unique advertising identifier, the user's intention to get pregnant, and the when the user was having her period.

36. Thereafter, the Federal Trade Commission ("FTC") issued a Complaint, *In the Matter of Flo Health, Inc*. Commission File No. 1923133, to Defendant advising that it had reason to believe that Defendant violated the provisions of the Federal Trade Commission Act. *See* **Exhibit 1**.

37. Specifically, the FTC Complaint found that Defendant's privacy policies in effect between August 28, 2017 and February 19, 2019, stated that Defendant "may share certain" personal data with third parties, but only for purposes of operating and servicing the Flo App. The privacy polices defined "personal data" broadly to include "information about your health" but also promised that any information shared with third parties "exclude[ed] information regarding your marked cycles, pregnancy, systems, notes and other information that is entered by you and that you do not elect to share." The privacy policies additionally promised that third parties could not use the Flo App users' personal information "for any other purpose except to provide services in connection with the App." *See id*. at ¶¶ 14-15.

38. In addition, privacy policies in effect between May 28, 2018 and February 19, 2019, promised that Defendant would not disclose "any data related to health" to either AppsFlyer or Flurry and also promised that Facebook, Google, and Fabric would only receive "non-personally identifiable information," "Personal Data like devise identifiers," or "devise identifiers." *See id. at* ¶¶ 16.

39. However, despite Defendant's own privacy polices providing otherwise

and the term of use of the various third parties restricting the app developer from collecting certain restricted data (including health data) since the data once collected would not be restricted by the third party, private health related information of Flo App users was nonetheless disclosed to these third parties to use in an unrestricted manner. *See id* at ¶¶ 20-22.

40. After an FTC's investigation, the Commission issued a decision and order with the following provisions: (1) a provision which prohibits Defendant from making false or deceptive statements regarding the extent to which Defendant collects, maintains, users or discloses certain private personal information; (2) a provision which requires Defendant to "ask" third-parties that received the personal information of the users to destroy the information; (3) a provision which requires that Defendant provide notice to users and the public that it shared certain information about users' periods and pregnancies with third parties; (4) a provision that, before disclosing any consumer's health information to a third party, Defendant must provide notice and obtain express affirmative consent; (5) a "Compliance Review" conducted within 180 days after entry of the January 13, 2021 Proposed Order; (6) a requirement that Defendant cooperate with the Compliance Review and certified compliance. *See* **Exhibit 2** at pp. 3-9.

41. A Joint Statement of Commissioner Rohit Chopra and Commissioner Rebecca Kelly Slaughter was issued which concurred in part and dissented in part to the FTC's decision and order. Importantly, the following was noted:

> In addition to requiring Flo to improve its privacy practices, the FTC's proposed order directs Flo to notify its users of this serious breach. Notice confers a number of benefits in cases like this one. Consumers deserve to know when a company made false privacy promises, so they can modify their usage or switch services. Notice also informs how consumers review a service, and whether they will recommend it to others. Finally, notice accords consumers the dignity of knowing what happened. For all these reasons, the

> Commission should presumptively seek notice provisions in privacy and data security matters, **especially in matters that do not include redress for victims.**

See **Exhibit 3** at p. 1 (emphasis added).

42. Additionally, the Joint Statement of Commissioner Rohit Chopra and Commissioner Rebecca Kelly Slaughter noted its disappointed in the Commission for "not using all of its tools to hold accountable those who abuse and misuse personal data" stating that Defendant should have also been held accountable for violating the Health Breach Notification Rules which requires vendors of unsecured health information, including mobile health apps, to notify users and the FTC if there has been a unauthorized disclosure.. *See id*. at p. 1.

43. Invasion of privacy has been recognized as a common law tort for over a century. *Matera v. Google Inc*., 15-CV-0402, 2016 WL 5339806, at *10 (N.D. Cal, Sept. 23, 2016) (citing Restatement (Second) of Torts §§ 652A-I for the proposition "that the right to privacy was first accepted by an American court in 1905, and 'a right to privacy is now recognized in the great majority of the American jurisdictions that have considered the question'"). *Id*. As Justice Brandeis explained in his seminal article, The Right to Privacy, "[t]he common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others." Samuel D. Warren & Louis Brandeis, The Right to Privacy, 4 HARV. L. REV. 193, 198 (1890). The Second Restatement of Torts recognizes the same privacy rights through its tort of intrusion upon seclusion, explaining that "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy." Restatement (Second) of Torts § 652B (1977).

44. The Supreme Court has similarly recognized the primacy of privacy rights, explaining that the Constitution operates in the shadow of a "right to privacy

older than the Bill of Rights." *Griswold v. Connecticut*, 381 U.S. 479, 486 (1965).

45. The Supreme Court explicitly recognized the reasonable expectation of privacy an individual has in her cell phone, and the personal data generated therefrom, in its opinion in *Carpenter v. United States*, 138 S. Ct. 2206 (2018). There, the Court held that continued access to an individual's cell phone location data constituted a search under the Fourth Amendment, and that the third-party doctrine (which obviates Fourth Amendment protections when a party knowingly provides information that is the subject of the search to third-parties) did not apply to such data. Critical to the Court's analysis was the fact that:

> a cell phone—almost a "feature of human anatomy[]"—tracks nearly exactly the movements of its owner.…A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales….Accordingly, when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user.

Id. at 2218 (internal citations omitted).

46. It is precisely because of devices' capacity for "near perfect surveillance" that courts have consistently held that time-honored legal principles recognizing a right to privacy in one's affairs naturally apply to online monitoring.

47. California amended its constitution in 1972 to specifically enumerate a right to privacy in its very first section. *See* Cal. Const. Art. I, § 1.

Factual Allegations as to Plaintiff

48. In 2017, Plaintiff Jennifer Chen downloaded Defendant's Flo App to her mobile device and thereafter frequently utilized the app on an ongoing and continuous basis.

49. Plaintiff Chen has provided Defendant with her intimate health data, including questions about her health and wellness and menstruation cycle in

response to Defendant's survey questions and has continued to provide intimate health information since she downloaded the app in 2017.

50. Plaintiff Chen believed that her intimate health information would stay private and that the private health information would not be disclosed to third parties as Defendant advised her information would remain provide and because she never provided her consent to disclose her personal health data.

51. However, in violation of Plaintiff Chen's privacy, Defendant disclosed Plaintiff's intimate health details without her knowledge or consent to third parties.

52. Plaintiff Chen would not have used the Flo App if she had known that her information would be shared with third parties.

53. The applicable statutes of limitation have been tolled as a result of Defendant's knowing and active concealment of the fact herein. Thus, Plaintiff and member of the putative Classes could not, with due diligence, have discovered the full scope of Defendant's conduct.

V. CLASS ALLEGATIONS

54. Plaintiff brings this class action lawsuit individually and on behalf of the proposed Classes under Rule 23 of the Federal Rules of Civil Procedure.

> **Nationwide Class**: All persons residing in the United States of America who used the Flo App.
>
> **California Subclass**: All person residing in California who used the Flo App.

55. Excluded from the Classes are the following individuals: officers and directors of Defendant and its parents, subsidiaries, affiliates, and any entity in which Defendant has a controlling interest; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

56. Plaintiff reserves the right to modify or amend the definitions of the

proposed Class before the Court determines whether certification is appropriate.

57. Numerosity. The members of the class are so numerous that a joinder of all members is impracticable. While the exact number of class members is unknown to Plaintiff at this time, the Defendant reports its app has been chosen by over 150 million women.[4]

58. Typicality. Plaintiff's claims are typical of the claims of the class members because, among other things, Plaintiff sustained similar injuries to that of Class Members as a result of Defendant's uniform wrongful conduct, and their legal claims all arise from the same events and wrongful conduct by Defendant.

59. Adequacy. Plaintiff will fairly and adequately protect the interests of the Class Members. Plaintiff's interests do not conflict with the interests of the Class Members and Plaintiff has retained counsel experienced in complex class action cases to prosecute this case on behalf of the Class.

60. Commonality. Common questions of law and fact exist as to all class members and predominate over any questions solely affecting individual members of the Class, including the following:

i. Whether Defendant engaged in the activities referenced herein;

ii. Whether Defendant collected Plaintiff and the Class member's personal data;

iii. Whether Defendant provided Plaintiff's personal data to third parties;

iv. Whether Defendant sold Plaintiff's personal data for profit;

v. Whether Defendant adequately disclosed its policy of providing personal data to third parties;

vi. Whether Defendant's collection and storage of Plaintiff's and the Class

---

[4] https://play.google.com/store/apps/details?id=org.iggymedia.periodtracker&hl=en_US&gl=US

and members' personal data in the manner alleged violated federal, state and local laws, or industry standards;

vii. Whether Defendant engaged in unfair, unlawful, or deceptive practices by providing personal data to third parties;

viii. Whether Defendant violated consumer protection and privacy statues applicable to Plaintiff and members of the Class;

ix. Whether Defendant acted negligently in failing to properly safeguard Plaintiff's and Class Members' personal data;

x. Whether Defendant's acts and practices complained of herein amount to egregious breaches of social norms; and

xi. The nature of the relief, including equitable relief, to which Plaintiff and Class Members are entitled.

61. Ascertainability. Class Members can easily be identified by an examination and analysis of the business records maintained by Defendant, among other records within Defendant's possession, custody, or control.

62. Predominance. The common issues of law and fact identified above predominate over any other questions affecting only individual members of the Class. The Class issues fully predominate over any individual issue because no inquiry into individual conduct is necessary; all that is required is a narrow focus on Defendant's conduct.

63. Superiority. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since a joinder of all members is impracticable. Furthermore, as damages suffered by Class Members may be relatively small, the expense and burden of individual litigation make it impossible for class members to individually redress the wrongs done to them. Individualized litigation also presents a potential for inconsistent or contradictory judgments, and increases the delay and expense presented by the complex legal and factual issues of the case to all parties and the court system. By contrast, the class action device

presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

64. Accordingly, this class action is properly brought and should be maintained as a class action because questions of law or fact common to Class Members predominate over any questions affecting only individual members, and because a class action is superior to other available methods for fairly and efficiently adjudicating this controversy.

65. This class action is also properly brought and should be maintained as a class action because Plaintiffs seek injunctive relief and declaratory relief on behalf of the Class Members on grounds generally applicable to the proposed Class. Certification is appropriate because Defendant has acted or refused to act in a manner that applies generally to the proposed Class, making final declaratory or injunctive relief appropriate.

FIRST CAUSE OF ACTION

Invasion of Privacy and Violation of the California Constitution, Art. 1, § 1

(On Behalf of Plaintiff and the Class and Subclass)

66. Plaintiff re-alleges and incorporates by reference each and every allegation contained elsewhere in this Complaint as if fully set forth herein.

67. Plaintiff and Class members have a legally protected privacy interest in their private and personal information that is collected by Defendant, and are entitled to the protection of their property and information against unauthorized access.

68. Defendant unlawfully invaded the privacy rights of Plaintiff and Class members by (a) failing to adequately secure their private and personal information from disclosure to unauthorized parties for improper purposes despite a promise to do so; (b) disclosing their private, and personal information to unauthorized parties in a manner that is highly offensive to a reasonable person; and (c) disclosing their private and personal information to unauthorized parties without the informed and clear consent of Plaintiff and Class members. This invasion into the privacy interest

of Plaintiff and Class members is serious and substantial.

69. Plaintiff and Class members reasonable expected that their personal data would be protected and secure from unauthorized parties, and that their private and personal information would not be disclosed to any unauthorized parties or disclosed for any improper purpose.

70. The reasonableness of such expectations of privacy is supported by Defendant's unique position to monitor Plaintiff's and Class members' behavior through their access to Plaintiff's and Class members' private mobile devices. It is further supported by the surreptitious, highly-technical, and non-intuitive nature of Defendant's tracking.

71. Defendant intentionally intruded on and into Plaintiff's and Class members' solitude, seclusion, right of privacy, or private affairs by intentionally designing the app (as well as all SDKs identified in this Complaint) to surreptitiously obtain, improperly gain knowledge of, review, and/or retain Plaintiff's and Class members' activities through the monitoring technologies and activities described herein.

72. These intrusions are highly offensive to a reasonable person, because they disclosed sensitive and confidential information about the user health, constituting an egregious breach of social norms. This is evidenced by, inter alia, centuries of common law, state and federal statutes and regulations, legislative commentaries, enforcement actions undertaken by the FTC, industry standards and guidelines, and scholarly literature on consumers' reasonable expectations.

73. Further, the extent of the intrusion cannot be fully known, as the nature of privacy invasion involves sharing Plaintiff's and Class members' personal information with potentially countless third-parties, known and unknown, for undisclosed and potentially unknowable purposes, in perpetuity.

74. Plaintiff and Class members were harmed by the intrusion into their private affairs as detailed throughout this Complaint.

75. Defendant's actions and conduct complained of herein were a substantial factor in causing the harm suffered by Plaintiff and Class members.

76. As a result of Defendant's actions, Plaintiff and Class members seek injunctive relief, in the form of Defendant's cessation of tracking practices in violation of state law, and ordered destruction of all personal data obtained in violation of state law.

77. As a result of Defendant's actions, Plaintiff and Class members seek nominal and punitive damages in an amount to be determined at trial. Plaintiff and Class members seek punitive damages because Defendant's actions—which were malicious, oppressive, willful—were calculated to injure Plaintiff and Class members and made in conscious disregard of Plaintiff's and Class members' rights. Punitive damages are warranted to deter Defendant from engaging in future misconduct.

SECOND CAUSE OF ACTION

Intrusion upon Seclusion

(On Behalf of Plaintiff and the Class and Subclass)

78. Plaintiff re-alleges and incorporates by reference each and every allegation contained elsewhere in this Complaint as if fully set forth herein.

79. Plaintiff and Class members reasonable expected that their personal data would be protected and secure from unauthorized parties, and that their private and personal information would not be disclosed to any unauthorized parties or disclosed for any improper purpose.

80. The reasonableness of such expectations of privacy is supported by Defendant's unique position to monitor Plaintiff's and Class members' behavior through their access to Plaintiff's and Class members' private mobile devices. It is further supported by the surreptitious, highly-technical, and non-intuitive nature of Defendant's tracking.

81. Defendant intentionally intruded on and into Plaintiff's and Class members' solitude, seclusion, or private affairs by intentionally designing the Flo App to obtain, improperly gain knowledge of, review, and/or retain Plaintiff's and Class members' activities through the monitoring technologies and activities described herein.

82. These intrusions are highly offensive to a reasonable person. This is evidenced by, *inter alia,* California Supreme Court precedent (most recently and forcefully articulated in the *Carpenter* opinion), legislation enacted by Congress, rules promulgated, and enforcement actions undertaken by the FTC, and countless studies, op-eds, and articles decrying location tracking. Further, the extent of the intrusion cannot be fully known, as the nature of privacy invasion involves sharing Plaintiff's and Class members' personal information with potentially countless third-parties, known and unknown, for undisclosed and potentially unknowable purposes, in perpetuity.

83. Plaintiff and Class Members were harmed by the intrusion into their private affairs as detailed throughout this Complaint.

84. Defendant's actions and conduct complained of herein were a substantial factor in causing the harm suffered by Plaintiff and Class Members.

85. As a result of Defendant's actions, Plaintiff and Class Members seek injunctive relief, in the form of Defendant's cessation of tracking practices in violation of state law, and ordered destruction of all personal data obtained in violation of state law.

86. Plaintiff and Class members also seek nominal and punitive damages in an amount to be determined at trial. Plaintiff and Class members seek punitive damages because Defendant's actions—which were malicious, oppressive, willful—were calculated to injure Plaintiff and made in conscious disregard of Plaintiff's rights. Punitive damages are warranted to deter Defendant from engaging in future misconduct.

THIRD CAUSE OF ACTION

Violation of the California Unfair Competition Law,

Cal. Bus. & Prof. Code §§ 17200, *et seq.*

(On Behalf of Plaintiff and the Class and Subclass)

87. Plaintiff re-alleges and incorporates by reference each and every allegation contained elsewhere in this Complaint as if fully set forth herein.

88. Defendant is subject to California's Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, *et seq*. The UCL provides, in pertinent part: "Unfair competition shall mean and include unlawful, unfair or fraudulent business practices…"

"Unfair" Prong

89. The UCL prohibits "unfair competition," which is broadly defined as including "any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising and any act prohibited by Chapter 1 (commencing with Section 17500) of Part 3 of Division 7 of the Business and Professions Code." Bus. & Prof. Code §17200.

90. Defendant's business practices, described herein, violated the "unfair" prong of the UCL in that their conduct is substantially injurious to consumers, offends public policy, and is immoral, unethical, oppressive, and unscrupulous, as the gravity of the conduct outweighs any alleged benefits. Defendant's tracking, collect, and selling of the Flo App users' personal identifying and health information for advertising purposes is of no benefit to the Flo App users.

91. Defendant has made material misrepresentations and omissions, both directly and indirectly, related to the privacy-invasive and unlawful behaviors and practices detailed herein.

92. As such, Defendant has engaged in unfair or deceptive acts in violation of the UCL.

93. Defendant's unfair acts allege herein deceived and misled App users.

Defendant has taken advantage of the lack of knowledge, ability, experience, or capacity of consumers to the detriment of those consumers.

94. Defendant's conduct also injures competing app developers, software designers and website operators that do not engage in the same unfair and unethical behavior.

95. Defendant's violations were, and are, willful, deceptive, unfair, and unconscionable. Defendant is aware of the violations but have failed to adequately and affirmatively take steps to cure the misconduct.

"Fraudulent" Prong

96. Under the "fraudulent" prong, a business practice is prohibited if it is likely to mislead or deceive a reasonable consumer or, where the business practice is aimed at a particularly susceptible audience, a reasonable member of that target audience. *See Lavie v. Proctor & Gamble Co.,* 105 Cal.App.4th 496, 506-07 (2003).

97. The UCL authorizes a civil enforcement action against "[a]ny person who engages, has engaged, or proposes to engage in unfair competition." Bus. & Prof. Code §17203. "[P]erson" includes "natural persons, corporations, firms, partnerships, joint stock companies, associations and other organizations of persons." *Id.* §17201.

98. Defendant intentionally misleads and deceives Flo App users to believe Defendant adheres to privacy-protected norms as well as through own privacy policies.

99. When users download the Flo App, Defendant and its SDK partners surreptitiously collect and sell the users' personal identifying information and profile them for behavioral and contextual targeted advertising.

100. Plaintiff and Class members acted reasonably when they downloaded the Flo App, which they believed to be beneficial in helping with their wellbeing.

101. Plaintiff and Class members lost money or property as a result of Defendant's UCL violations because (a) they would not have downloaded the Flo

App absent Defendant's representations and omission of a warning that their information would be tracked, collected, and sold for contextual and behavioral advertising.

"Unlawful" Prong

102. Defendant's business practices, described herein, violated the "unlawful" prong of the UCL by violating California's Constitutional Right to Privacy; Intrusion Upon Seclusion, Cal. Bus. & Prof. Code § 22575; the California Consumer Privacy Act (2018) (CCPA), Cal. Civ. Code § 1798.120(c), and the Health Information Technology for Clinical and Economic Health Act (HITECH).

103. Such conduct is ongoing and continues to date.

104. Defendant's conduct further violates other applicable California and Federal regulations as alleged herein.

105. Plaintiff and Class Members are likely to continue to be damaged by Defendant's deceptive practices thus injunctive relief enjoining Defendant's deceptive practices is proper.

106. There were reasonably available alternatives to further Defendant's legitimate business interests, other than the conduct described herein.

107. Defendant's practices are therefore unfair, unlawful, and fraudulent under Section 17200 *et. seq.* of the California Civil Code.

FOURTH CAUSE OF ACTION

Negligent Misrepresentation

Cal. Civ. Code §§ 1709-1710

(On Behalf of Plaintiff and the Class and Subclass)

108. Plaintiff re-alleges and incorporates by reference each and every allegation contained elsewhere in this Complaint as if fully set forth herein.

109. Defendant resented that information collected by the Flo App would be kept private, however Defendant improperly shared personal health data with third parties, including whether users were ovulating.

110. The misrepresentations were communicated to Plaintiff and the Class members through the Flo App privacy policies.

111. The misrepresentations concerned material facts that influenced Plaintiff and the Class members' downloading of the App.

112. Following publication of a February 22, 2019 *Wall Street Journal* report that it was able to intercept unencrypted identifying health information transmitted by the Flo App to Facebook, Defendant received more than 300 complaint from Flo App users about the unauthorized disclosure of health information to Facebook. More than 100 Flow App users asked Responded to delete their accounts and/or data or told the company they were deleting, or would delete, the Flo App. *See* **Exhibit 1** at pp. 5-6.

113. At the time Defendant made the misrepresentations, Defendant knew or should have known that the misrepresentations were false, or Defendant made the misrepresentations without knowledge of their truth or veracity.

114. Plaintiff and the Class members reasonably, justifiably, and detrimentally relied on the misrepresentations and, as a proximate result thereof, have and will continue to suffer damages.

FIFTH CAUSE OF ACTION

Unjust Enrichment

(On Behalf of Plaintiff and the Class and Subclass)

115. Plaintiff re-alleges and incorporates by reference each and every allegation contained elsewhere in this Complaint as if fully set forth herein.

116. By collecting, storing, and using Plaintiff's and Class members' personal data without their permission, Defendant was unjustly enriched at the expense of Plaintiff and Class members. It would be inequitable, unjust, and unconscionable for Defendant to retain the benefit it obtained from using Plaintiff's and Class member's personal data for advertising purposes.

117. Plaintiff seeks disgorgement of all proceeds, profits, benefits, and other

compensation obtained by Defendant from their improper and unlawful use and collection of Plaintiff's and the Class members' personal data, as well as all other appropriate relief permitted by law of unjust enrichment, including reasonable attorneys' fees and costs of suit.

SIXTH CAUSE OF ACTION

Violation of the Comprehensive Computer Data Access and Fraud Act ("CDAFA")

Cal. Penal Code § 502

(On Behalf of Plaintiff and the Class and Subclass)

118. Plaintiff re-alleges and incorporates by reference each and every allegation contained elsewhere in this Complaint as if fully set forth herein.

119. The California Legislature enacted the California Computer Data Access and Fraud Act, Cal. Penal Code § 502 ("CDAFA") to "expand the degree of protection afforded. . . from tampering, interference, damage, and unauthorized access to (including the extraction of data from) lawfully created computer data and computer systems," finding and declaring that "the proliferation of computer technology has resulted in a concomitant proliferation of . . . forms of unauthorized access to computers, computer systems, and computer data," and that "protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals. . . ." Cal. Penal Code § 502(a).

120. Plaintiff's and members of the Class' devices on which they unitized the Flo App including their computers, smart phones, and tablets constitute "computers, computer systems, and/or computer networks" within the meaning of the CDAFA.

121. Defendant violated § 502(c)(1)(B) of the CDAFA by knowingly accessing and without permission accessing Plaintiff's and Class members' devices in order to obtain their personal information, including their device and location data,

and in order for Defendant to share that data with third parties, in violation of Flo App users' reasonable expectations of privacy in their devices and data.

122. Defendant violated Cal. Penal Code § 502(c)(2) by knowingly and without permission accessing, taking and using Plaintiff's and the Class members' personally identifiable information.

123. The computers and mobile devices that Plaintiff and Class members used to when accessing Defendant's Flo App all have and operate "computer services" within the meaning of the CDAFA. Defendant violated §§ 502(c)(3) and (7) of the CDAFA by knowingly and without permission accessing and using those devices and computer services, or causing them to be accessed and used, *inter alia* in connection with Defendant's sharing of information with third parties.

124. Defendant violated §§ 502(c)(6) and (c)(13) of the CDAFA by knowingly and without permission providing and/or assisting in providing third parties.

125. Under California Penal Code § 502(b)(10) a "Computer contaminant" is defined as "any set of computer instructions that are designed to ... record, or transmit information within computer, computer system, or computer network without the intent or permission of the owner of the information."

126. Defendant violated California Penal Code § 502(c)(8) by knowingly and without permission introducing a computer contaminant into the transactions between Plaintiff and the Class members and websites; including but not limited to the code that intercepted Plaintiff's and the Class Members' private and personal data.

127. As a direct and proximate result of Defendant's unlawful conduct within the meaning of California Penal Code § 502, Defendant caused loss to Plaintiff and the Class members in an amount to be proven at trial, including that Plaintiff and the Class members were injured by the loss of value of their personal information. Plaintiff and the Class members are also entitled to recover their

reasonable attorneys' fees under California Penal Code § 502(e)(2).

128. Plaintiff and the Class members seek compensatory damages in accordance with California Penal Code § 502(e)(1), in an amount to be proven at trial, and injunctive or other equitable relief.

129. Plaintiff and Class members have suffered irreparable and incalculable harm and injuries from Defendant's violations. The harm will continue unless Defendant is enjoined from further violations of this section. Plaintiff and Class members have no adequate remedy at law.

130. Plaintiff and the Class members are entitled to punitive or exemplary damages pursuant to Cal. Penal Code § 502(e)(4) because Defendant's violations were willful and, upon information and belief, Defendant is guilty of oppression, fraud, or malice as defined in Cal. Civil Code § 3294.

131. Plaintiff and Class members have also suffered irreparable injury from these unauthorized acts of disclosure, their persona, private, and sensitive health information have been collected, viewed, accessed, stored, and used by Defendant and third parties, and have not been destroyed, and due to the continuing threat of such injury, have no adequate remedy at law, entitled Plaintiff to injunctive relief.

SEVENTH CAUSE OF ACTION

Violation of the Federal Wiretap Act

18 U.S.C §§ 2510, *et seq.*

(On Behalf of Plaintiff and the Classes)

132. Plaintiff re-alleges and incorporates by reference each and every allegation contained elsewhere in this Complaint as if fully set forth herein.

133. The Wiretap Act generally prohibits the intentional "interception" of "wire, oral, or electronic communication." 18 U.S.C. § 2511(1).

134. By knowingly accessing Plaintiff's and Class members' devices without their permission to obtain their personal information, including their device and location data, for Defendant to share that data with third parties, in violation of

Flo App users' reasonable expectations of privacy in their devices and data, Defendant intentionally intercepted and/or endeavored to intercept the contents of "electronic communication," in violation of 18 U.S.C. § 2511(1).

135. No party to the electronic communications alleged herein consented to Defendant's interception or use of the contents of the electronic communications. Nor could they – Defendant never sought to obtain Plaintiff's or the Class members' consent, and each interception occurred concurrently while they used the Flo App on their mobile devise. Moreover, Defendant was not a party to any of the communications sent and/or received by Plaintiff and members of the Class, which were sent direct to third parties via the SDK embedded into the Flo App.

136. Plaintiff and the Class suffered harm as a result of Defendant's violations of the Wiretap Act, and therefore seek (a) preliminary, equitable, and declaratory relief as may be appropriate, (b) the sum of the actual damages suffered and the profits obtained by Defendant as a result of its unlawful conduct, or statutory damages as authorized by 18 U.S.C. § 2520(2)(B), whichever is greater, (c) punitive damages, and (d) costs and attorneys' fee.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all Class members proposed in this Complaint, respectfully requests that the Court enter a judgment in his favor and against Defendant, as follows:

A. Determining that this action may be maintained as a class action under Rule 23 of the Federal Rules of Civil Procedure and appointing and her Counsel to represent the Classes;

B. Finding Defendant's conduct was unlawful as alleged herein;

C. Enjoining Defendant from engaging in the wrongful conduct complained of herein;

D. Requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

E. Awarding Plaintiff and Class members actual damages, compensatory damages, punitive damages, statutory damages, and statutory penalties, in an amount to be determined;

F. Awarding Plaintiff and Class members costs of suit and attorneys' fees, as allowable by law; and

G. Granting such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury of all issues so triable.

DATED: February 26, 2021

Respectfully submitted,

/s/ Ronald A. Marron
Ronald A. Marron
LAW OFFICES OF RONALD A. MARRON
RONALD A. MARRON
ron@consumersadvocates.com
ALEXIS M. WOOD
alexis@consumersadvocates.com
KAS L. GALLUCCI
kas@consumersadvocates.com
651 Arroyo Drive
San Diego, California 92103
Telephone: (619) 696-9006
Facsimile: (619) 564-6665

Attorney for Plaintiff and the Proposed Class