1923133

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Lina Khan, Chair**
Noah Joshua Phillips
Rohit Chopra
Rebecca Kelly Slaughter
Christine S. Wilson

In the Matter of **FLO HEALTH, INC.**	**DOCKET NO. C-4747**

COMPLAINT

The Federal Trade Commission ("FTC"), having reason to believe that Flo Health, Inc., a corporation ("Respondent"), has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Flo Health, Inc. ("Flo Health") is a Delaware corporation with its principal office or place of business at 1013 Centre Road, Suite 403-B, Wilmington, Delaware 19805.

2. Respondent 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").

3. Millions of women use the Flo App, giving Respondent details of their menstruations and gynecological health on the promise that the app will help predict ovulation and aid in pregnancy and childbirth. These users trust Respondent with intimate details of their reproductive health because Respondent repeatedly promised to protect the information and keep it secret. Indeed, Respondent's privacy policies stated, time and again, that Respondent would not share users' health details with anyone.

4. In fact, beginning in 2016, Respondent handed users' health information out to numerous 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"). And Respondent took no action to limit what these companies could do with the users' information. Rather, they merely agreed to each company's standard terms of service. By doing so, Respondent gave these third parties the ability to use Flo App users' personal health information expansively, including for advertising.

5. Respondent shared women's personal health information with these third parties for years, while at the same time promising them privacy. It was not until February 2019, when the Wall Street Journal revealed the practice, that Respondent halted sharing the data. Indeed, Respondent stopped sharing users' health information with Facebook the day after the exposé.

6. Upon learning that Respondent had turned some data related to their menstruations, pregnancies, and childbirths over to these third parties, hundreds of users wrote to Respondent, stating that they were "outraged," "incredibly upset," "disturbed," "appalled," and "very angry." Indeed, they felt "victimized" and "violated" by Respondent's actions.

7. The acts and practices of Respondent alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

Flo App

8. Since at least 2016, Respondent has made the Flo App available to users for free download from the Apple App Store and the Google Play Store. In the product description available on the Apple App Store, Respondent describes the Flo App as "a smart and simple period tracker, helpful pregnancy week by week app, accurate ovulation and fertility calendar and PMS symptoms tracker for women all over the world."

9. The Flo App is one of the most popular health and fitness apps available to consumers. Since 2016, more than 100 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 App Store in over 30 countries.

10. During the relevant time period, Respondent contracted with dozens of third-party firms to provide, among other things, various marketing and analytics services in connection with the Flo App. These firms included Facebook's analytics division, Google's analytics division, Fabric, AppsFlyer, and Flurry. Respondent did not contractually limit how these third parties could use data they received from the Flo App. In fact, the Terms of Service governing the agreements permitted the third parties to use the data for their own purposes.

11. Respondent encourages women to input vast quantities of health information into the Flo App: "Log your menstruation days in a handy period calendar, ovulation and fertility tracker, schedule menstrual cycle reminders, record moods and PMS symptoms, use a due date calculator, follow a pregnancy calendar ...." By doing so, Respondent tells users, you can "take full control of your health."

12. By encouraging millions of women to input extensive information about their bodies and mental and physical health, Respondent has collected personal information about consumers, including name, email address, date of birth, place of residence, dates of menstrual cycles, when pregnancies started and ended, menstrual and pregnancy-related symptoms, weight, and temperature.

Respondent's Repeated Deceptive Statements to Flo App Users About Health Data

13. Between 2017 and 2019, Respondent repeatedly promised users that the Flo App would keep their health data private, and that Respondent would only use Flo App users' data to provide the Flo App's services. Many users entrusted Respondent with their health information in part because they believed that Respondent would treat it according to Respondent's privacy policies.

14. Specifically, in privacy policies in effect between August 28, 2017 and February 19, 2019, Respondent explained that it "may share certain" personal data with third parties, but only for purposes of operating and servicing the Flo App. The privacy policies defined "personal data" broadly to include "information about your health." However, the privacy policies then asserted that any information shared with third parties "**exclud[ed] information regarding your marked cycles, pregnancy, symptoms**, notes and other information that is entered by you and that you do not elect to share." (emphasis added).

15. In the privacy policies described in Paragraph 14, Respondent also promised that third parties could not use Flo App users' personal information "for any other purpose except to provide services in connection with the App."

16. In addition to stating that Respondent would not share "information regarding your marked cycles, pregnancy, [or] symptoms ..." with any third parties (as described in Paragraph 14), privacy policies in effect between May 28, 2018 and February 19, 2019 specifically promised that Respondent would not disclose "any data related to health" to either AppsFlyer or Flurry.

A. "AppsFlyer is a mobile marketing platform. We may share certain non-identifiable information about you and some Personal Data **(but never any data related to health)** in order to carry out marketing activities and provide you better and more targeted, tailor-made service." (emphasis added)

B. "We may share certain non-identifiable information about you and some Personal Data **(but never any data related to health)** with Flurry." (emphasis added)

17. The privacy policies described in Paragraph 16 also singled out Facebook, Google, and Fabric, claiming that these third parties would only receive "non-personally identifiable information," "Personal Data like device identifiers," or "device identifiers." Specifically, Respondent's privacy policies stated as follows:

A. "We use Facebook Analytics and Google Analytics tools to track installs of our App. Normally, Facebook and Google collect **only non-personally identifiable information,** though some **Personal Data like device identifiers** may be transferred to Facebook ...." (emphasis added).

B. "**Fabric may use device identifiers** that are stored on your mobile device and allow us to analyze your use of the App in order to improve our app feature [sic]." (emphasis added).

For Years, Respondent Disclosed Health Data About Millions of App Users to Facebook, Google, and Other Third Parties

18. Like most app developers, Respondent tracks "Standard App Events," records of routine app functions, such as launching or closing the app, as well as "Custom Apps Events," records of user-app interactions unique to the Flo App. For example, when a user enters menstruation dates, Respondent records the user's interaction with that feature as a Custom App Event. Respondent analyzes Custom App Events to improve the Flo App's functionality and identify which features are likely to interest new users.

19. Respondent gave each Custom App Event a descriptive title. For example, when a user enters the week of her pregnancy, Respondent records the Custom App Event "R_PREGNANCY_WEEK_CHOSEN." When a user selects a feature to receive menstruation reminders in the "wanting to get pregnant branch" of the app, Respondent records the Custom App Event "P_ACCEPT_PUSHES_PERIOD." Consequently, many of Respondent's Custom App Events convey information about users' menstruation, fertility, or pregnancies.

20. Despite its repeated representations between 2017 and 2019 that it would keep users' health data secret, Respondent disclosed health information to various third parties. In fact, as far back as June 2016, Respondent integrated into the Flo App software development tools, known as software development kits ("SDKs"), from the numerous third-party marketing and analytics firms mentioned above, 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. By including sensitive health information in the titles of the Custom App Events, Respondent conveyed the health information of millions of users to these third parties for years. This directly contradicted Respondent's statements in its privacy policies that it would not divulge such information. Specifically, Respondent disclosed Custom App Event information to:

A. Facebook from June 2016 to February 2019;

B. Flurry from June 2016 to February 2019;

C. Fabric from November 2016 to February 2019;

D. AppsFlyer from May 2018 to February 2019; and

E. Google from September 2018 to February 2019.

21. Besides breaking promises to Flo App users, Respondent's disclosures violated several of the third parties' own terms of service or use—terms to which Respondent had agreed:

A. Facebook's Business Tools Terms stated: "**You will not share Customer Data with us that you know or reasonably should know ... includes health**, financial information, or other categories of sensitive information (including any information defined as sensitive under applicable law)." (emphasis added).

B. AppsFlyer's Terms of Use stated: "**AppsFlyer strictly prohibits you from using the Services to collect or otherwise enable the collection of any Restricted Data**. You hereby warrant that you shall not configure the Codes or Services to collect any Restricted Data through the Services." The Terms of Use defined "Restricted Data" to include "**any health information**." (emphasis added).

22. Despite representing in the privacy policies described in Paragraphs 14 and 15 that it would restrict how third parties could use Flo App users' personal data, Respondent merely agreed to these third parties' stock terms of service, several of which permitted the third party to use any information obtained from Flo App users for the third party's own purposes, including, in certain cases, for advertising and product improvement:

A. Facebook's Business Tools Terms stated: "We use [aggregated] Event Data to personalize the features and content (including ads and recommendations) we show people on and off our Facebook Company Products .... We may also use Event Data ... for research and development purposes, and to ... improve the Facebook Company Products." That "Event Data" includes Custom App Events.

B. Google Analytics's Terms of Service stated: "Google and its wholly owned subsidiaries may retain and use ... information collected in [Flo Health's] use of the service."

C. AppsFlyer's Terms of Use stated: "You hereby allow AppsFlyer to collect, store, use and process Customer Data," where "Customer Data" was defined to include "data concerning the characteristics and activities" of app users.

D. The Fabric Software and Services Agreement stated: "[Flo Health] acknowledges and agrees that Google [Fabric] may use Usage Data for its own business purposes," where "Usage Data" was defined to mean "all information, data and other content, not including any [identifying data], received by Google related to [Flo Health]'s use of the Fabric Technology.

23. As a result, at least one of these third parties (Facebook) used Flo App event data (which Facebook did not know included users' personal and health data) for its own purposes, including its own research and development purposes.

24. 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 Wall Street Journal reported that this information included a unique advertising identifier, the user's intention to get pregnant, and when the user was having her period.

25. Following publication of the *Wall Street Journal's* story, Respondent received more than 300 complaints from Flo App users about the unauthorized disclosures of health information to Facebook. For example, users stated:

A. "I'm absolutely [sic] disgusted at this invasion of my most personal information."

B. "This is private personal data and I feel disgusted that you are now making this data available to third parties."

C. "Why would you EVER think it is ok to share that personal, private information with a third [sic] party?"

26. More than 100 Flo App users asked Respondent to delete their accounts and/or data or told the company they were deleting, or would delete, the Flo App.

Respondent's Violation of the Privacy Shield Principles

27. Respondent has been a participant in the EU-U.S. Privacy Shield ("Privacy Shield") and the U.S.-Swiss Privacy Shield framework since August 12, 2018. In privacy policies effective from August 6, 2018 through the present, Respondent has represented that it participates in the EU-U.S. Privacy Shield framework and the U.S.-Swiss Privacy Shield framework. Specifically, since August 6, 2018, Respondent's privacy policies have stated: "[W]e comply with the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the EU and Switzerland to the United States. We have certified to the Department of Commerce that we adhere to the Privacy Shield Principles."

28. The Department of Commerce ("Commerce") and the European Commission negotiated the Privacy Shield to provide a mechanism for companies to transfer personal data from the European Union to the United States in a manner consistent with the requirements of European Union law on data protection. Enacted in 1995, the European Union Data Protection Directive (the "Directive") set forth European Union requirements for the protection of personal data. Among other things, it required European Union Member States to implement legislation that prohibits the transfer of personal data outside the European Union, with exceptions, unless the European Commission has made a determination that the recipient jurisdiction's laws ensure the protection of such personal data. This determination commonly referred to as meeting the European Union's "Adequacy Standard."

29. The European Union has since enacted a new data protection regime, the General Data Protection Regulation ("GDPR"), which took effect as of May 25, 2018, and contains similar provisions on data transfers. The GDPR explicitly recognizes European Commission adequacy determinations in effect as of that date. Unlike the Directive, the GDPR is directly applicable and generally does not require member states to enact implementing legislation.

30. To satisfy the European Union Adequacy Standard for certain commercial transfers, Commerce and the European Commission negotiated the Privacy Shield, which the European Commission determined was adequate by written decision in July 2016, and took effect August 1, 2016. Thus, the Privacy Shield allows for the lawful transfer of personal data from the European Union to those companies in the United States that participate in Privacy Shield.

31. The Swiss-U.S. Privacy Shield Framework is identical to the EU-U.S. Privacy Shield Framework and is consistent with the requirements of the Swiss Federal Act on Data Protection.

32. To join the EU-U.S. and/or Swiss-U.S. Privacy Shield Framework, a company must self-certify to Commerce that it complies with the Privacy Shield Principles, and to related requirements that have been deemed to meet the European Union's Adequacy Standard. Participating companies must annually re-certify their compliance.

33. The Privacy Shield expressly provides that, while decisions by organizations to "enter the Privacy Shield are entirely voluntary, effective compliance is compulsory: organizations that self-certify to the Department and publicly declare their commitment to adhere to the Principles **must comply fully** with the Principles." (emphasis added).

34. Companies under the jurisdiction of the FTC are eligible to join the EU-U.S. and/or Swiss-U.S. Privacy Shield Framework. Both frameworks warn companies that claim to have self-certified to the Privacy Shield Principles that failure to comply or otherwise to "fully implement" the Privacy Shield Principles "is enforceable under Section 5 of the Federal Trade Commission Act."

Respondent's Failure to Provide Adequate Notice for Third-Party Use of Health Information for Advertising and Other Purposes

35. Privacy Shield Principle 1, "Notice," requires organizations to inform individuals about, among other things, "the type or identity of third parties to which it discloses personal information, and the purposes for which it does so." Principle 1(a)(vi). It provides further: "This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party." Principle 1(b).

36. Respondent did not provide notice in clear and conspicuous language about the purposes for which it disclosed health information to third parties. When users in the European Union, Switzerland, Norway, Lichtenstein, and Iceland opened the Flo App for the first time, they were greeted by a "Welcome" screen that provided that by using the Flo App, the user consented to Respondent's aforementioned privacy policies and terms of use.

37. However, as described in Paragraphs 20-23, Respondent disclosed users' health information to numerous third parties authorized to use the data for advertising (among other uses). At no point did Respondent inform users that their health data could be used for these third parties' purposes.

Respondent's Failure to Provide Adequate Choice for Third-Party Use of Health Information for Advertising, Product Improvement, and Other Purposes

38. Privacy Shield Principle 2, "Choice," requires organizations to "offer individuals the opportunity to choose (opt out) whether their personal information is ... to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by the individuals." Principle 2(a).

39. The Choice Principle specifies further: "Individuals must be provided with clear, conspicuous, and readily available mechanisms to exercise choice." *Id.*

40. This Principle also requires opt-in consent for disclosures of "sensitive information *(i.e.,* personal information specifying medical or health conditions ...)." Principle 2(c). Specifically, Principle 2(c) requires that "organizations must obtain affirmative express consent (opt in) from individuals if such information is to be [] disclosed to a third party ..." *Id.*

41. Respondent did not offer users the opportunity to opt out of whether their personal information would be used for a materially different purpose than the purposes for which it was originally collected or subsequently authorized. Specifically, Respondent told App users that their health information would only be used to provide the Flo App functions. Respondent did not offer Flo App users the opportunity to opt out of the use of their health information by third parties for advertising, product improvement, and other purposes.

42. Respondent did not obtain Flo App users' affirmative express opt-in consent for disclosures of health information to third parties, including Facebook, Google, Flurry, Fabric, and AppsFlyer. To the contrary, as described in Paragraphs 13-14 and 16, Respondent reassured Flo App users that the Flo App would **not** disclose health information to third parties.

43. Respondent did not offer individuals a clear, conspicuous, and readily available mechanism to exercise choice. The aforementioned privacy policy provided misleading information, which prevented users from exercising choice.

Respondent's Failure to Provide for Accountability for Onward Transfers

44. Privacy Shield Principle 3, "Accountability for Onward Transfer," requires organizations that transfer personal data to a third party acting as an agent to, among other things, "(i) transfer such data only for limited and specified purposes, (ii) ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles, [and] (iii) take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's obligations under the Principles." Principle 3(b).

45. To the extent Respondent considered AppsFlyer, Fabric, Facebook, Flurry, and Google to be its agents, Respondent violated Principle 3 because it did not transfer Flo App users' health data to third parties acting as Respondent's agents only for limited and specified purposes. To the contrary, as described in Paragraphs 20 and 22, Respondent transferred health information to numerous third parties that Respondent considered its agents under broad contracts that permitted use of the data received for wide-ranging purposes, including the third parties' advertising and product improvement.

46. Respondent also violated Principle 3 because it did not obligate third parties that Respondent considered its agents to provide the same level of privacy protection as is required by the Principles. Specifically, Respondent transferred users' health information to AppsFlyer, Fabric, Facebook, Flurry, and Google, without requiring these third parties to provide the same level of privacy protection for this data as is required by the Principles.

47. Respondent also violated Principle 3 because it did not take reasonable and appropriate steps to ensure processing of users' information consistent with the Principles. Specifically, as described in Paragraph 22, Respondent did not require third parties it considered agents, including Facebook, Google, Fabric, and AppsFlyer, to sign any contract acknowledging that they could or would receive Flo App users' health information or requiring processing consistent with the sensitivity of this information. To the contrary, as described in Paragraph 21, Respondent agreed to terms of service that specifically prohibited disclosures of health information to Facebook and AppsFlyer.

48. As a result, these third parties were not even aware that they had received Flo App users' health data and, therefore, could not process the data in a manner consistent with its sensitivity.

Respondent's Failure to Abide by the Principle of Purpose Limitation

49. Privacy Shield Principle 5, "Data Integrity and Purpose Limitation," provides, in part: "An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual." Principle 5(a).

50. Respondent collected health information from Flo App users for the purpose of providing the Flo App's functions. By disclosing Flo App users' health information to third parties under contracts that permitted those third parties to use the data for advertising, product improvement and other purposes, Respondent processed Flo App users' health information in a way that was incompatible with the purposes for which it has been collected.

Count I
Privacy Misrepresentation – Disclosures of Health Information

51. As described in Paragraphs 13-14 and 16, Respondent represented, directly or indirectly, expressly or by implication, that the Flo App would not disclose, without consumers' consent, their health information to third parties in general, and to AppsFlyer and Flurry in particular.

52. In fact, as set forth in Paragraph 20, Respondent did disclose consumers' health information to Facebook, Google, Fabric, Flurry, and AppsFlyer. Therefore, the representations set forth in Paragraph 51 are false or misleading.

Count II
Privacy Misrepresentation – Disclosures Beyond Identifiers

53. As described in Paragraph 17, Respondent represented, directly or indirectly, expressly or by implication, that it would only disclose non-personally identifiable information, device identifiers, and personal data "like device identifiers" to Fabric, Google, and Facebook.

54. In fact, as set forth in Paragraph 20, Respondent did not only disclose non-personally identifiable information, device identifiers, and personal data "like device identifiers" to Fabric, Google, and Facebook. Respondent also conveyed users' health information to Google,

Facebook, and Fabric. Therefore, the representations set forth in Paragraph 53 are false or misleading.

Count III
Privacy Misrepresentation – Failure to Limit Third-Party Use

55. As described in Paragraphs 14-15, Respondent represented, directly or indirectly, expressly or by implication, that third parties could not use Flo App users' personal information "for any other purpose except to provide services in connection with the App."

56. In fact, as set forth in Paragraph 22, third parties could use Flo App users' personal information for purposes other than providing services in connection with the app. Respondent entered into agreements with third parties Facebook, Google, AppsFlyer, and Fabric that permitted them to use Flo App users' personal information for the third parties' own purposes, including for advertising and product improvement. Furthermore, as set forth in Paragraph 23, from June 2016 to February 2019, at least one third party (Facebook) used the Flo App users' personal information for its own purposes, including its own research and development purposes. Therefore, the representations set forth in Paragraph 55 are false or misleading.

Count IV
Misrepresentation Regarding Notice

57. As described in Paragraph 27, Respondent has represented, directly or indirectly, expressly or by implication, that it adheres to the Privacy Shield Framework Principles, including the principle of Notice.

58. In fact, as described in Paragraphs 36-37, Respondent did not adhere to the Privacy Shield Principle of Notice. Therefore, the representation set forth in Paragraph 57 is false or misleading.

Count V
Misrepresentation Regarding Choice

59. As described in Paragraph 27, Respondent has represented, directly or indirectly, expressly or by implication, that it adheres to the Privacy Shield Framework Principles, including the principle of Choice.

60. In fact, as described in Paragraphs 41-43, Respondent did not adhere to the Privacy Shield Principle of Choice. Therefore, the representation set forth in Paragraph 59 is false or misleading.

Count VI
Misrepresentation Regarding Accountability for Onward Transfers

61. As described in Paragraph 27, Respondent has represented, directly or indirectly, expressly or by implication, that it adheres to the Privacy Shield Framework Principles, including the principle of Accountability for Onward Transfers.

62. In fact, as described in Paragraphs 45-48, Respondent did not adhere to the Privacy Shield Principle of Accountability for Onward Transfers. Therefore, the representation set forth in Paragraph 61 is false or misleading.

Count VII
Misrepresentation Regarding Data Integrity and Purpose Limitation

63. As described in Paragraph 27, Respondent has represented, directly or indirectly, expressly or by implication, that it adheres to the Privacy Shield Framework Principles, including the principle of Data Integrity and Purpose Limitation.

64. In fact, as described in Paragraph 50, Respondent did not adhere to the Privacy Shield Principle of Data Integrity and Purpose Limitation. Therefore, the representation set forth in Paragraph 63 is false or misleading.

Violations of Section 5

65. The acts and practices of Respondent as alleged in this complaint constitute unfair or deceptive acts or practices, in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act.

THEREFORE, the Federal Trade Commission this 17th day of June 2021, has issued this complaint against Respondent.

By the Commission.

April J. Tabor
Acting Secretary

SEAL: