

Complaint

IN THE MATTER OF

FLO HEALTH, INC.CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF SECTION 5 OF THE FEDERAL
TRADE COMMISSION ACT

Docket No. C-4747; File No. 192 3133
Complaint, June 17, 2021 – Decision, June 17, 2021

This consent order addresses Flo Health, Inc.’s mobile application called the Flo Period & Ovulation Tracker, which collects and stores menstruation and fertility information about millions of users worldwide. The complaint alleges that Flo Health violated of Section 5(a) of the Federal Trade Commission Act by misrepresenting their use and disclosure of consumer’s personal information, and compliance with the Privacy Shield Principles of Notice, Choice, Accountability for Onward Transfers, and Purpose Limitation. The consent order requires Flo Health to ask any party other than Flo Health, its service providers, or subcontractors, that has received “Health Information” about “Covered App Users” to destroy such information; and prohibits Flo Health from making false or deceptive statements regarding: (1) the purposes for which Flo Health or any entity to whom it discloses, collects, maintains, or uses personal information, including identifiable health information; (2) the extent to which consumers may exercise control over Flo Health’s access, collection, maintenance, use, disclosure, or deletion of such information; (3) the extent to which Flo Health complies with any privacy, security, or compliance program, including the Privacy Shield; and (4) the extent to which Flo Health collects, maintains, uses, discloses, deletes, or permits or denies access to any Covered Information, or the extent to which Flo Health protects the availability, confidentiality, or integrity of Covered Information.

Participants

For the *Commission*: *Elisa Jillson and Miles Plant.*

For the *Respondents*: *David Kantrowitz and Brenda Sharton, Goodwin Procter LLP.*

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

Complaint

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

Complaint

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)

Complaint

- 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:

Complaint

- 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"

Complaint

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.”

Complaint

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.”

Complaint

**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.

Complaint

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.

Complaint

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.

Complaint

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.

Decision and Order

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.

DECISION

The Federal Trade Commission (“Commission”) initiated an investigation of certain acts and practices of the Respondent named in the caption. The Commission’s Bureau of Consumer Protection (“BCP”) prepared and furnished to Respondent a draft Complaint. BCP proposed to present the draft Complaint to the Commission for its consideration. If issued by the Commission, the draft Complaint would charge the Respondent with violations of the Federal Trade Commission Act.

Respondent and BCP thereafter executed an Agreement Containing Consent Order (“Consent Agreement”). The Consent Agreement includes: 1) statements by Respondent that it neither admits nor denies any of the allegations in the Complaint, except as specifically stated in this Decision and Order, and that only for purposes of this action, it admits the facts necessary to establish jurisdiction; and 2) waivers and other provisions as required by the Commission’s Rules.

Decision and Order

The Commission considered the matter and determined that it had reason to believe that Respondent has violated the Federal Trade Commission Act, and that a Complaint should issue stating its charges in that respect. The Commission accepted the executed Consent Agreement and placed it on the public record for a period of thirty (30) days for the receipt and consideration of public comments. The Commission duly considered any comments received from interested persons pursuant to Section 2.34 of its Rules, 16 C.F.R. § 2.34. Now, in further conformity with the procedure prescribed in Rule 2.34, the Commission issues its Complaint, makes the following Findings, and issues the following Order:

Findings

1. The Respondent is Flo Health, Inc. (“Flo Health”), a Delaware corporation with its principal office or place of business at 1013 Centre Road, Suite 403-B, Wilmington, Delaware 19805.
2. The Commission has jurisdiction over the subject matter of this proceeding and over the Respondent, and the proceeding is in the public interest.

ORDER**Definitions**

For purposes of this Order, the following definitions apply:

- A. “Clearly and Conspicuously” means that a required disclosure is difficult to miss (*i.e.*, easily noticeable) and easily understandable by ordinary consumers, including in all of the following ways:
 1. In any communication that is solely visual or solely audible, the disclosure must be made through the same means through which the communication is presented. In any communication made through both visual and audible means, such as a television advertisement, the disclosure must be presented simultaneously in both the visual and audible portions of the communication even if the representation requiring the disclosure (“triggering representation”) is made through only one means.
 2. A visual disclosure, by its size, contrast, location, the length of time it appears, and other characteristics, must stand out from any accompanying text or other visual elements so that it is easily noticed, read, and understood.
 3. An audible disclosure, including by telephone or streaming video, must be delivered in a volume, speed, and cadence sufficient for ordinary consumers to hear it easily and understand it.

Decision and Order

4. In any communication using an interactive electronic medium, such as the Internet or software, the disclosure must be unavoidable.
 5. The disclosure must use diction and syntax understandable to ordinary consumers and must appear in each language in which the triggering representation appears.
 6. The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications.
 7. The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication.
 8. When the representation or sales practice targets a specific audience, such as children, the elderly, or the terminally ill, “ordinary consumers” includes reasonable members of that group.
- B. “Covered App User” means any individual who downloaded and used Respondent’s mobile application Flo Period & Ovulation Tracker between June 30, 2016 and February 23, 2019.
- C. “Covered Incident” means any instance in which Respondent discloses Health Information to a Third Party without first receiving that consumer’s affirmative express consent.
- D. “Covered Information” means information from or about an individual consumer, including but not limited to: (a) a first and last name; (b) a physical address; (c) an email address or other online contact information, such as a user identifier or a screen name; (d) a telephone number; (e) a Social Security number; (f) a driver’s license or other government-issued identification number; (g) a financial institution account number; (h) credit or debit card information; (i) a persistent identifier, such as a customer number held in a “cookie,” a static Internet Protocol (“IP”) address, a mobile device ID, or processor serial number; (j) Health Information; or (k) any information combined with any of (a) through (j) above.
- E. “Health Information” means individually identifiable information from or about an individual consumer relating to health, including but not limited to information concerning fertility, menstruation, sexual activity, pregnancy, and childbirth.
- F. “Respondent” means Flo Health, a corporation, and its successors and assigns.
- G. “Third Party” means any individual or entity other than: (1) Respondent; (2) a service provider of Respondent that: (i) uses or receives Covered Information collected by or on behalf of Respondent for and at the direction of the Respondent and no other individual or entity, (ii) does not disclose the data, or any

Decision and Order

individually identifiable information derived from such data, to any individual or entity other than Respondent or a subcontractor to such service provider bound to data processing terms no less restrictive than terms to which the service provider is bound, and (iii) does not use the data for any other purpose; or (3) any entity that uses Covered Information only as reasonably necessary: (i) to comply with applicable law, regulation, or legal process, (ii) to enforce Respondent's terms of use, or (iii) to detect, prevent, or mitigate fraud or security vulnerabilities.

Provisions**I. Prohibition against Misrepresentations about Information Privacy**

IT IS ORDERED that Respondent, Respondent's officers, agents, employees, and attorneys, and all other persons in active concert or participation with either of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with any product or service must not misrepresent in any manner, expressly or by implication:

- A. the purposes for which Respondent or any entity to whom it discloses Covered Information collects, maintains, uses, or discloses Covered Information;
- B. the extent to which consumers may exercise control over Respondent's collection, maintenance, use, disclosure, or deletion of Covered Information, and the steps a consumer must take to implement such controls;
- C. the extent to which Respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy, security, or any other compliance program sponsored by a government or any self-regulatory or standard-setting organization, including the EU-U.S. Privacy Shield and the U.S.-Swiss Privacy Shield framework; and
- D. the extent to which Respondent collects, maintains, uses, discloses, deletes, or permits or denies access to any Covered Information, or the extent to which Respondent protects the availability, confidentiality, or integrity of any Covered Information.

II Data Deletion

IT IS FURTHER ORDERED that, on or before thirty (30) days after the date of the filing of this Order, Respondent and Respondent's officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, must instruct any Third Party that has received Health Information from Respondent belonging to any Covered App User to destroy such information.

Decision and Order

III. Notice to Users

IT IS FURTHER ORDERED that on or before fourteen (14) days after the date of the filing of this Order, Respondent must post Clearly and Conspicuously on Respondent's website, <https://flo.health/>, an exact copy of the notice attached hereto as Exhibit A ("Notice") and email the Notice to all Covered App Users, *provided however*, that if Respondent does not have email information for any Covered App User, Respondent must send the Notice to that Covered App User through Respondent's primary means of communicating with that user (such as a notification within Respondent's mobile application). Respondent shall not include with the Notice any other information, documents, or attachments.

IV. Notice and Affirmative Express Consent

IT IS FURTHER ORDERED that Respondent and Respondent's officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, in connection with any product or service, prior to disclosing any consumer's Health Information to any Third Party, must:

- A. Clearly and Conspicuously disclose to the consumer, separate and apart from any "privacy policy," "terms of use" page, or other similar document: (1) the categories of Health Information that will be disclosed to such Third Parties, (2) the identities of such Third Parties, and (3) all purposes for Respondent's disclosure of such Health Information, including how it may be used by each Third Party; and
- B. obtain the consumer's affirmative express consent.

V. Compliance Review

IT IS FURTHER ORDERED that, within 180 days after the issuance date of this Order, Respondent must obtain an outside review of certain of its practices (the "Compliance Review"):

- A. The Compliance Review must be completed by a qualified, objective, independent third-party professional, who: (1) uses procedures and standards generally accepted in the profession; (2) conducts an independent review of compliance with the EU-U.S. Privacy Shield Framework Principles (the "Principles"), attached hereto as Exhibit B; and (3) retains all documents relevant to the Compliance Review for five (5) years after completion and will provide such documents to the Commission within ten (10) days of receipt of a written request from a representative of the Commission. No documents may be withheld on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney-client privilege, statutory exemption, or any similar claim.
- B. Respondent shall provide the Associate Director of Enforcement for the Bureau of Consumer Protection at the Commission with the name, affiliation, and resume of

Decision and Order

each person selected to conduct the Compliance Review, which the Associate Director shall have the authority to approve in his sole discretion.

- C. The reporting period for the Compliance Review must cover the first 180 days after the issuance date of the Order.
- D. The Compliance Review must (1) determine whether Respondent has maintained compliance with the Principles attached hereto as Exhibit B; (2) determine whether Respondent's privacy practices are consistent with its privacy policy; (3) determine whether Respondent adequately informs individuals about the mechanisms through which they may pursue complaints regarding Respondent's privacy practices; (4) identify any gaps or weaknesses in the privacy practices assessed; and (5) identify specific evidence (including, but not limited to, documents reviewed, sampling and technical testing performed, and interviews conducted) examined to make such determinations and identifications, and explain why the evidence examined is sufficient to justify the findings. No finding of the Compliance Review shall rely solely on assertions or attestations by Respondent's management. The Compliance Review shall be signed by the lead professional who performs the review and shall state that he or she conducted an independent review of Respondent's privacy practices, and did not rely solely on assertions or attestations by Respondent's management.
- E. Unless otherwise directed by a Commission representative in writing, Respondent must submit the Compliance Review to the Commission within ten (10) days after the Compliance Review has been completed via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: "In re Flo Health, Inc., LLC, FTC File No. 1923133."

VI. Cooperation with Compliance Reviewer

IT IS FURTHER ORDERED that Respondent, whether acting directly or indirectly, in connection with the Compliance Review required by Provision V of this Order, must disclose all material facts to the individual(s) conducting the Compliance Review (the "Reviewer"), and must not misrepresent in any manner, expressly or by implication, any fact material to the Reviewer's determination whether Respondent (1) has maintained compliance with the Principles attached hereto as Exhibit B; (2) has engaged in privacy practices consistent with its privacy policy; (3) adequately informs individuals about the mechanisms through which they may pursue complaints regarding Respondent's privacy practices; or (4) has any gaps or weaknesses in its privacy practices.

VII. Certification

IT IS FURTHER ORDERED that, in connection with Provisions I through VI of this Order, Respondent must:

Decision and Order

- A. Within 180 days after the issuance date of this Order, provide the Commission with a certification from a senior corporate manager, or, if no such senior corporate manager exists, a senior officer of Respondent responsible for Respondent's privacy practices that Respondent: (1) has established, implemented, and maintained the requirements of this Order; and (2) is not aware of any material noncompliance that has not been (a) corrected or (b) disclosed to the Commission. The certification must be based on the personal knowledge of the senior corporate manager, senior officer, or subject matter experts upon whom the senior corporate manager or senior officer reasonably relies in making the certification.
- B. Unless otherwise directed by a Commission representative in writing, submit the certification to the Commission pursuant to this Order via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: "In re Flo Health, Inc., LLC, FTC File No. 1923133."

VIII. Covered Incident Reports

IT IS FURTHER ORDERED that Respondent, within thirty (30) days after that Respondent's discovery of a Covered Incident, must submit a report to the Commission. The report must include, to the extent possible:

- A. The date, estimated date, or estimated date range when the Covered Incident occurred;
- B. A description of the facts relating to the Covered Incident, including the causes and scope of the Covered Incident, if known;
- C. The number of consumers whose information was affected;
- D. The acts that Respondent has taken to date to remediate the Covered Incident and protect Health Information from further disclosure, exposure or access, and protect affected individuals from identity theft or other harm that may result from the Covered Incident; and
- E. A representative copy of any materially different notice sent by Respondent to consumers or to any U.S. federal, state, or local government entity.

Unless otherwise directed by a Commission representative in writing, all Covered Incident reports to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: "In re Flo Health, Inc., LLC, FTC File No. 1923133."

Decision and Order

IX. Acknowledgments of the Order

IT IS FURTHER ORDERED that Respondent obtain acknowledgments of receipt of this Order:

- A. Respondent, within ten (10) days after the effective date of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.
- B. For five (5) years after the issuance date of this Order, Respondent, must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees having managerial responsibilities for conduct related to the subject matter of the Order, and all agents and representatives who participate in conduct related to the subject matter of the Order; and (3) any business entity resulting from any change in structure as set forth in the Provision titled Compliance Reports and Notices. Delivery must occur within ten (10) days after the effective date of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.
- C. From each individual or entity to which Respondent delivered a copy of this Order, Respondent must obtain, within thirty (30) days, a signed and dated acknowledgment of receipt of this Order.

X. Compliance Reports and Notices

IT IS FURTHER ORDERED that Respondent makes timely submissions to the Commission:

- A. Sixty (60) days after the issuance date of this Order, and annually thereafter for five (5) more years, Respondent must submit a compliance report, sworn under penalty of perjury, in which Respondent must: (a) identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission, may use to communicate with Respondent; (b) identify all of Respondent's businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (c) describe the activities of each business, including the services offered, what Covered Information is collected, and how Covered Information is used and disclosed to third parties; (d) describe in detail whether and how Respondent is in compliance with each Provision of this Order, including a discussion of all of the changes Respondent made to comply with the Order; and (e) provide a copy of each Acknowledgment of the Order obtained pursuant to this Order, unless previously submitted to the Commission.
- B. Respondent must submit a compliance notice, sworn under penalty of perjury, within fourteen (14) days of any change in: (a) any designated point of contact or (b) the structure of Respondent or any entity Respondent has any ownership

Decision and Order

interest in or control directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order.

- C. Respondent must submit notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against Respondent within fourteen (14) days of its filing.
- D. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: “I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____” and supplying the date, signatory’s full name, title (if applicable), and signature.
- E. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: In re Flo Health, Inc., a corporation.

XI. Recordkeeping

IT IS FURTHER ORDERED that Respondent must create certain records for twenty (20) years after the issuance date of the Order, and retain each such records for five (5) years, unless otherwise specified below. Specifically, Respondent must create and retain the following records:

- A. accounting records showing the revenues from all goods or services sold, the costs incurred in generating those revenues, and resulting net profit or loss;
- B. personnel records showing, for each person providing services in relation to any aspect of the Order, whether as an employee or otherwise, that person’s: name, addresses, telephone numbers, job title or position, dates of service, and (if applicable) the reason for termination;
- C. copies or records of all consumer complaints and refund requests sent to Respondent, and any response;
- D. all records necessary to demonstrate full compliance with each provision of this Order, including all submissions to the Commission;
- E. a copy of each unique advertisement or other marketing material making a representation subject to this Order;

Decision and Order

- F. a copy of each widely disseminated representation by Respondent that describes the extent to which Respondent maintains or protects the privacy, security and confidentiality of any Covered Information, including any representation concerning a change in any website or other service controlled by Respondent that relates to the privacy, security, and confidentiality of Covered Information;
- G. for five (5) years after the date of preparation of the Compliance Review required by this Order, all materials relied upon to prepare the Compliance Review, whether prepared by or on behalf of Respondent, including all plans, reports, studies, reviews, audits, audit trails, policies, training materials, assessments, and any other materials concerning Respondent's compliance with related Provisions of this Order, for the compliance period covered by the Compliance Review.

XII. Compliance Monitoring

IT IS FURTHER ORDERED that, for the purpose of monitoring Respondent's compliance with this Order:

- A. Within ten (10) days of receipt of a written request from a representative of the Commission, Respondent must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury, and produce records for inspection and copying.
- B. For matters concerning this Order, representatives of the Commission are authorized to communicate directly with Respondent. Respondent must permit representatives of the Commission to interview anyone affiliated with Respondent who has agreed to such an interview. The interviewee may have counsel present.
- C. The Commission may use all other lawful means, including posing through its representatives as consumers, suppliers, or other individuals or entities, to Respondent or any individual or entity affiliated with Respondent, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

XIII. Order Effective Dates

IT IS FURTHER ORDERED that this Order is final and effective upon the date of its publication on the Commission's website (ftc.gov) as a final order. This Order will terminate twenty (20) years from the date of its issuance (which date may be stated at the end of this Order, near the Commission's seal), or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

- A. Any Provision in this Order that terminates in less than twenty (20) years;

Decision and Order

- B. This Order if such complaint is filed after the Order has terminated pursuant to this Provision.

Provided, further, that if such complaint is dismissed or a federal court rules that Respondent did not violate any provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order will terminate according to this Provision as though the complaint had never been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

Exhibit A

Dear [Customer]:

Between June 1, 2016 and February 23, 2019, the company that makes the Flo Period & Ovulation Tracker app sent an identifying number related to you and information about your period and pregnancy to companies that help us measure and analyze trends, usage, and activities on the app, including the analytics divisions of Facebook, Flurry, Fabric, and Google. No information was shared with the social media divisions of these companies. We did not share your name, address, or birthday with anyone at any time.

We do not currently, and will not, share any information about your health with any company unless we get your permission. We recently entered into a settlement with the Federal Trade Commission, the nation's consumer protection agency, to resolve allegations that sharing this information was inconsistent with the promises we made to you. Learn more about the settlement at [\[to be determined\]](#). This page also includes links to resources for consumers to help them evaluate the risks and benefits of sharing information with health apps.

If you have any questions or concerns, please contact us at privacy@flo.health.

Decision and Order

Exhibit B**EU-U.S. PRIVACY SHIELD FRAMEWORK PRINCIPLES
ISSUED BY THE U.S. DEPARTMENT OF COMMERCE****I. OVERVIEW**

1. While the United States and the European Union share the goal of enhancing privacy protection, the United States takes a different approach to privacy from that taken by the European Union. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self-regulation. Given those differences and to provide organizations in the United States with a reliable mechanism for personal data transfers to the United States from the European Union while ensuring that EU data subjects continue to benefit from effective safeguards and protection as required by European legislation with respect to the processing of their personal data when they have been transferred to non-EU countries, the Department of Commerce is issuing these Privacy Shield Principles, including the Supplemental Principles (collectively “the Principles”) under its statutory authority to foster, promote, and develop international commerce (15 U.S.C. § 1512). The Principles were developed in consultation with the European Commission, and with industry and other stakeholders, to facilitate trade and commerce between the United States and European Union. They are intended for use solely by organizations in the United States receiving personal data from the European Union for the purpose of qualifying for the Privacy Shield and thus benefitting from the European Commission’s adequacy decision¹. The Principles do not affect the application of national provisions implementing Directive 95/46/EC (“the Directive”) that apply to the processing of personal data in the Member States. Nor do the Principles limit privacy obligations that otherwise apply under U.S. law.
2. In order to rely on the Privacy Shield to effectuate transfers of personal data from the EU, an organization must self-certify its adherence to the Principles to the Department of Commerce (or its designee) (“the Department”). While decisions by organizations to thus 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. In order to enter the Privacy Shield, an organization must (a) be subject to the investigatory and enforcement powers of the Federal Trade Commission (the “FTC”), the Department of Transportation or another statutory body that will effectively ensure compliance with the Principles (*other U.S. statutory bodies recognized by the EU may be included as an annex in the future*); (b) publicly declare its commitment to comply with the Principles; (c) publicly

¹ Provided that the Commission Decision on the adequacy of the protection provided by the EU-U.S. Privacy Shield applies to Iceland, Liechtenstein and Norway, the Privacy Shield Package will cover both the European Union, as well as these three countries. Consequently, references to the EU and its Member States will be read as including Iceland, Liechtenstein and Norway.

Decision and Order

disclose its privacy policies in line with these Principles; and (d) fully implement them. An organization's failure to comply is enforceable under Section 5 of the Federal Trade Commission Act prohibiting unfair and deceptive acts in or affecting commerce (15 U.S.C. § 45(a)) or other laws or regulations prohibiting such acts.

3. The Department of Commerce will maintain and make available to the public an authoritative list of U.S. organizations that have self-certified to the Department and declared their commitment to adhere to the Principles ("the Privacy Shield List"). Privacy Shield benefits are assured from the date that the Department places the organization on the Privacy Shield List. The Department will remove an organization from the Privacy Shield List if it voluntarily withdraws from the Privacy Shield or if it fails to complete its annual re-certification to the Department. An organization's removal from the Privacy Shield List means it may no longer benefit from the European Commission's adequacy decision to receive personal information from the EU. The organization must continue to apply the Principles to the personal information it received while it participated in the Privacy Shield, and affirm to the Department on an annual basis its commitment to do so, for as long as it retains such information; otherwise, the organization must return or delete the information or provide "adequate" protection for the information by another authorized means. The Department will also remove from the Privacy Shield List those organizations that have persistently failed to comply with the Principles; these organizations do not qualify for Privacy Shield benefits and must return or delete the personal information they received under the Privacy Shield.
4. The Department will also maintain and make available to the public an authoritative record of U.S. organizations that had previously self-certified to the Department, but that have been removed from the Privacy Shield List. The Department will provide a clear warning that these organizations are not participants in the Privacy Shield; that removal from the Privacy Shield List means that such organizations cannot claim to be Privacy Shield compliant and must avoid any statements or misleading practices implying that they participate in the Privacy Shield; and that such organizations are no longer entitled to benefit from the European Commission's adequacy decision that would enable those organizations to receive personal information from the EU. An organization that continues to claim participation in the Privacy Shield or makes other Privacy Shield-related misrepresentations after it has been removed from the Privacy Shield List may be subject to enforcement action by the FTC, the Department of Transportation, or other enforcement authorities.
5. Adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case law that creates conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent

Decision and Order

necessary to meet the overriding legitimate interests furthered by such authorization; or (c) if the effect of the Directive or Member State law is to allow exceptions or derogations, provided such exceptions or derogations are applied in comparable contexts. Consistent with the goal of enhancing privacy protection, organizations should strive to implement these Principles fully and transparently, including indicating in their privacy policies where exceptions to the Principles permitted by (b) above will apply on a regular basis. For the same reason, where the option is allowable under the Principles and/or U.S. law, organizations are expected to opt for the higher protection where possible.

6. Organizations are obligated to apply the Principles to all personal data transferred in reliance on the Privacy Shield after they enter the Privacy Shield. An organization that chooses to extend Privacy Shield benefits to human resources personal information transferred from the EU for use in the context of an employment relationship must indicate this when it self-certifies to the Department and conform to the requirements set forth in the Supplemental Principle on Self-Certification.
7. U.S. law will apply to questions of interpretation and compliance with the Principles and relevant privacy policies by Privacy Shield organizations, except where such organizations have committed to cooperate with European data protection authorities ("DPAs"). Unless otherwise stated, all provisions of the Principles apply where they are relevant.
8. Definitions:
 - a. "Personal data" and "personal information" are data about an identified or identifiable individual that are within the scope of the Directive, received by an organization in the United States from the European Union, and recorded in any form.
 - b. "Processing" of personal data means any operation or set of operations which is performed upon personal data, whether or not by automated means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure or dissemination, and erasure or destruction.
 - c. "Controller" means a person or organization which, alone or jointly with others, determines the purposes and means of the processing of personal data.
9. The effective date of the Principles is the date of final approval of the European Commission's adequacy determination.

Decision and Order

II. PRINCIPLES**1. NOTICE**

- a. An organization must inform individuals about:
 - i. its participation in the Privacy Shield and provide a link to, or the web address for, the Privacy Shield List,
 - ii. the types of personal data collected and, where applicable, the entities or subsidiaries of the organization also adhering to the Principles,
 - iii. its commitment to subject to the Principles all personal data received from the EU in reliance on the Privacy Shield,
 - iv. the purposes for which it collects and uses personal information about them,
 - v. how to contact the organization with any inquiries or complaints, including any relevant establishment in the EU that can respond to such inquiries or complaints,
 - vi. the type or identity of third parties to which it discloses personal information, and the purposes for which it does so,
 - vii. the right of individuals to access their personal data,
 - viii. the choices and means the organization offers individuals for limiting the use and disclosure of their personal data,
 - ix. the independent dispute resolution body designated to address complaints and provide appropriate recourse free of charge to the individual, and whether it is: (1) the panel established by DPAs, (2) an alternative dispute resolution provider based in the EU, or (3) an alternative dispute resolution provider based in the United States,
 - x. being subject to the investigatory and enforcement powers of the FTC, the Department of Transportation or any other U.S. authorized statutory body,
 - xi. the possibility, under certain conditions, for the individual to invoke binding arbitration,
 - xii. the requirement to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements, and
 - xiii. its liability in cases of onward transfers to third parties.

Decision and Order

- b. 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.

2. CHOICE

- a. An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (i) to be disclosed to a third party or (ii) 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. Individuals must be provided with clear, conspicuous, and readily available mechanisms to exercise choice.
- b. By derogation to the previous paragraph, it is not necessary to provide choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. However, an organization shall always enter into a contract with the agent.
- c. For sensitive information (*i.e.*, personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), organizations must obtain affirmative express consent (opt in) from individuals if such information is to be (i) disclosed to a third party or (ii) used for a purpose other than those for which it was originally collected or subsequently authorized by the individuals through the exercise of opt-in choice. In addition, an organization should treat as sensitive any personal information received from a third party where the third party identifies and treats it as sensitive.

3. ACCOUNTABILITY FOR ONWARD TRANSFER

- a. To transfer personal information to a third party acting as a controller, organizations must comply with the Notice and Choice Principles. Organizations must also enter into a contract with the third-party controller that provides that such data may only be processed for limited and specified purposes consistent with the consent provided by the individual and that the recipient will provide the same level of protection as the Principles and will notify the organization if it makes a determination that it can no longer meet this obligation. The contract shall provide that when such a determination is made the third party controller ceases processing or takes other reasonable and appropriate steps to remediate.
- b. To transfer personal data to a third party acting as an agent, organizations must: (i) transfer such data only for limited and specified purposes; (ii)

Decision and Order

ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; (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; (iv) require the agent to notify the organization if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles; (v) upon notice, including under (iv), take reasonable and appropriate steps to stop and remediate unauthorized processing; and (vi) provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request.

4. SECURITY

- a. Organizations creating, maintaining, using or disseminating personal information must take reasonable and appropriate measures to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data.

5. DATA INTEGRITY AND PURPOSE LIMITATION

- a. Consistent with the Principles, personal information must be limited to the information that is relevant for the purposes of processing.² 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. To the extent necessary for those purposes, an organization must take reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete, and current. An organization must adhere to the Principles for as long as it retains such information.
- b. Information may be retained in a form identifying or making identifiable³ the individual only for as long as it serves a purpose of processing within the meaning of 5a. This obligation does not prevent organizations from processing personal information for longer periods for the time and to the

² Depending on the circumstances, examples of compatible processing purposes may include those that reasonably serve customer relations, compliance and legal considerations, auditing, security and fraud prevention, preserving or defending the organization's legal rights, or other purposes consistent with the expectations of a reasonable person given the context of the collection.

³ In this context, if, given the means of identification reasonably likely to be used (considering, among other things, the costs of and the amount of time required for identification and the available technology at the time of the processing) and the form in which the data is retained, an individual could reasonably be identified by the organization, or a third party if it would have access to the data, then the individual is "identifiable."

Decision and Order

extent such processing reasonably serves the purposes of archiving in the public interest, journalism, literature and art, scientific or historical research, and statistical analysis. In these cases, such processing shall be subject to the other Principles and provisions of the Framework. Organizations should take reasonable and appropriate measures in complying with this provision.

6. ACCESS

- a. Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, or has been processed in violation of the Principles, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

7. RECOURSE, ENFORCEMENT AND LIABILITY

- a. Effective privacy protection must include robust mechanisms for assuring compliance with the Principles, recourse for individuals who are affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum such mechanisms must include:
 - i. readily available independent recourse mechanisms by which each individual's complaints and disputes are investigated and expeditiously resolved at no cost to the individual and by reference to the Principles, and damages awarded where the applicable law or private-sector initiatives so provide;
 - ii. follow-up procedures for verifying that the attestations and assertions organizations make about their privacy practices are true and that privacy practices have been implemented as presented and, in particular, with regard to cases of non-compliance; and
 - iii. obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.
- b. Organizations and their selected independent recourse mechanisms will respond promptly to inquiries and requests by the Department for information relating to the Privacy Shield. All organizations must respond expeditiously to complaints regarding compliance with the Principles referred by EU Member State authorities through the Department. Organizations that have chosen to cooperate with DPAs, including organizations that process human resources data, must respond directly to

Decision and Order

such authorities with regard to the investigation and resolution of complaints.

- c. Organizations are obligated to arbitrate claims and follow the terms as set forth in Annex I, provided that an individual has invoked binding arbitration by delivering notice to the organization at issue and following the procedures and subject to conditions set forth in Annex I.
- d. In the context of an onward transfer, a Privacy Shield organization has responsibility for the processing of personal information it receives under the Privacy Shield and subsequently transfers to a third party acting as an agent on its behalf. The Privacy Shield organization shall remain liable under the Principles if its agent processes such personal information in a manner inconsistent with the Principles, unless the organization proves that it is not responsible for the event giving rise to the damage.
- e. When an organization becomes subject to an FTC or court order based on non-compliance, the organization shall make public any relevant Privacy Shield-related sections of any compliance or assessment report submitted to the FTC, to the extent consistent with confidentiality requirements. The Department has established a dedicated point of contact for DPAs for any problems of compliance by Privacy Shield organizations. The FTC will give priority consideration to referrals of non-compliance with the Principles from the Department and EU Member State authorities, and will exchange information regarding referrals with the referring state authorities on a timely basis, subject to existing confidentiality restrictions.

Decision and Order

III. SUPPLEMENTAL PRINCIPLES**1. Sensitive Data**

- a. An organization is not required to obtain affirmative express consent (opt in) with respect to sensitive data where the processing is:
 - i. in the vital interests of the data subject or another person;
 - ii. necessary for the establishment of legal claims or defenses;
 - iii. required to provide medical care or diagnosis;
 - iv. carried out in the course of legitimate activities by a foundation, association or any other non-profit body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to the persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects;
 - v. necessary to carry out the organization's obligations in the field of employment law; or
 - vi. related to data that are manifestly made public by the individual.

2. Journalistic Exceptions

- a. Given U.S. constitutional protections for freedom of the press and the Directive's exemption for journalistic material, where the rights of a free press embodied in the First Amendment of the U.S. Constitution intersect with privacy protection interests, the First Amendment must govern the balancing of these interests with regard to the activities of U.S. persons or organizations.
- b. Personal information that is gathered for publication, broadcast, or other forms of public communication of journalistic material, whether used or not, as well as information found in previously published material disseminated from media archives, is not subject to the requirements of the Privacy Shield Principles.

3. Secondary Liability

- a. Internet Service Providers ("ISPs"), telecommunications carriers, and other organizations are not liable under the Privacy Shield Principles when on behalf of another organization they merely transmit, route, switch, or cache information. As is the case with the Directive itself, the Privacy Shield does not create secondary liability. To the extent that an organization is acting as a mere conduit for data transmitted by third parties and does not

Decision and Order

determine the purposes and means of processing those personal data, it would not be liable.

4. Performing Due Diligence and Conducting Audits

- a. The activities of auditors and investment bankers may involve processing personal data without the consent or knowledge of the individual. This is permitted by the Notice, Choice, and Access Principles under the circumstances described below.
- b. Public stock corporations and closely held companies, including Privacy Shield organizations, are regularly subject to audits. Such audits, particularly those looking into potential wrongdoing, may be jeopardized if disclosed prematurely. Similarly, a Privacy Shield organization involved in a potential merger or takeover will need to perform, or be the subject of, a “due diligence” review. This will often entail the collection and processing of personal data, such as information on senior executives and other key personnel. Premature disclosure could impede the transaction or even violate applicable securities regulation. Investment bankers and attorneys engaged in due diligence, or auditors conducting an audit, may process information without knowledge of the individual only to the extent and for the period necessary to meet statutory or public interest requirements and in other circumstances in which the application of these Principles would prejudice the legitimate interests of the organization. These legitimate interests include the monitoring of organizations’ compliance with their legal obligations and legitimate accounting activities, and the need for confidentiality connected with possible acquisitions, mergers, joint ventures, or other similar transactions carried out by investment bankers or auditors.

5. The Role of the Data Protection Authorities

- a. Organizations will implement their commitment to cooperate with European Union data protection authorities (“DPAs”) as described below. Under the Privacy Shield, U.S. organizations receiving personal data from the EU must commit to employ effective mechanisms for assuring compliance with the Privacy Shield Principles. More specifically as set out in the Recourse, Enforcement and Liability Principle, participating organizations must provide: (a)(i) recourse for individuals to whom the data relate; (a)(ii) follow up procedures for verifying that the attestations and assertions they have made about their privacy practices are true; and (a)(iii) obligations to remedy problems arising out of failure to comply with the Principles and consequences for such organizations. An organization may satisfy points (a)(i) and (a)(iii) of the Recourse, Enforcement and Liability Principle if it adheres to the requirements set forth here for cooperating with the DPAs.

Decision and Order

- b. An organization commits to cooperate with the DPAs by declaring in its Privacy Shield self-certification submission to the Department of Commerce (*see* Supplemental Principle on Self-Certification) that the organization:
 - i. elects to satisfy the requirement in points (a)(i) and (a)(iii) of the Privacy Shield Recourse, Enforcement and Liability Principle by committing to cooperate with the DPAs;
 - ii. will cooperate with the DPAs in the investigation and resolution of complaints brought under the Privacy Shield; and
 - iii. will comply with any advice given by the DPAs where the DPAs take the view that the organization needs to take specific action to comply with the Privacy Shield Principles, including remedial or compensatory measures for the benefit of individuals affected by any non-compliance with the Principles, and will provide the DPAs with written confirmation that such action has been taken.
- c. Operation of DPA Panels
 - i. The cooperation of the DPAs will be provided in the form of information and advice in the following way:
 - 1. The advice of the DPAs will be delivered through an informal panel of DPAs established at the European Union level, which will *inter alia* help ensure a harmonized and coherent approach.
 - 2. The panel will provide advice to the U.S. organizations concerned on unresolved complaints from individuals about the handling of personal information that has been transferred from the EU under the Privacy Shield. This advice will be designed to ensure that the Privacy Shield Principles are being correctly applied and will include any remedies for the individual(s) concerned that the DPAs consider appropriate.
 - 3. The panel will provide such advice in response to referrals from the organizations concerned and/or to complaints received directly from individuals against organizations which have committed to cooperate with DPAs for Privacy Shield purposes, while encouraging and if necessary helping such individuals in the first instance to use the in-house complaint handling arrangements that the organization may offer.
 - 4. Advice will be issued only after both sides in a dispute have had a reasonable opportunity to comment and to provide any evidence they wish. The panel will seek to deliver advice as quickly as this requirement for due process allows. As a

Decision and Order

general rule, the panel will aim to provide advice within 60 days after receiving a complaint or referral and more quickly where possible.

5. The panel will make public the results of its consideration of complaints submitted to it, if it sees fit.
 6. The delivery of advice through the panel will not give rise to any liability for the panel or for individual DPAs.
- ii. As noted above, organizations choosing this option for dispute resolution must undertake to comply with the advice of the DPAs. If an organization fails to comply within 25 days of the delivery of the advice and has offered no satisfactory explanation for the delay, the panel will give notice of its intention either to refer the matter to the Federal Trade Commission, the Department of Transportation, or other U.S. federal or state body with statutory powers to take enforcement action in cases of deception or misrepresentation, or to conclude that the agreement to cooperate has been seriously breached and must therefore be considered null and void. In the latter case, the panel will inform the Department of Commerce so that the Privacy Shield List can be duly amended. Any failure to fulfill the undertaking to cooperate with the DPAs, as well as failures to comply with the Privacy Shield Principles, will be actionable as a deceptive practice under Section 5 of the FTC Act or other similar statute.
- d. An organization that wishes its Privacy Shield benefits to cover human resources data transferred from the EU in the context of the employment relationship must commit to cooperate with the DPAs with regard to such data (*see* Supplemental Principle on Human Resources Data).
 - e. Organizations choosing this option will be required to pay an annual fee which will be designed to cover the operating costs of the panel, and they may additionally be asked to meet any necessary translation expenses arising out of the panel's consideration of referrals or complaints against them. The annual fee will not exceed USD 500 and will be less for smaller companies.

6. Self-Certification

- a. Privacy Shield benefits are assured from the date on which the Department has placed the organization's self-certification submission on the Privacy Shield List after having determined that the submission is complete.
- b. To self-certify for the Privacy Shield, an organization must provide to the Department a self-certification submission, signed by a corporate officer on behalf of the organization that is joining the Privacy Shield, that contains at least the following information:

Decision and Order

- i. name of organization, mailing address, e-mail address, telephone, and fax numbers;
- ii. description of the activities of the organization with respect to personal information received from the EU; and
- iii. description of the organization's privacy policy for such personal information, including:
 - 1. if the organization has a public website, the relevant web address where the privacy policy is available, or if the organization does not have a public website, where the privacy policy is available for viewing by the public;
 - 2. its effective date of implementation;
 - 3. a contact office for the handling of complaints, access requests, and any other issues arising under the Privacy Shield;
 - 4. the specific statutory body that has jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy (and that is listed in the Principles or a future annex to the Principles);
 - 5. name of any privacy program in which the organization is a member;
 - 6. method of verification (*e.g.*, in-house, third party) (*see* Supplemental Principle on Verification); and
 - 7. the independent recourse mechanism that is available to investigate unresolved complaints.
- c. Where the organization wishes its Privacy Shield benefits to cover human resources information transferred from the EU for use in the context of the employment relationship, it may do so where a statutory body listed in the Principles or a future annex to the Principles has jurisdiction to hear claims against the organization arising out of the processing of human resources information. In addition, the organization must indicate this in its self-certification submission and declare its commitment to cooperate with the EU authority or authorities concerned in conformity with the Supplemental Principles on Human Resources Data and the Role of the Data Protection Authorities as applicable and that it will comply with the advice given by such authorities. The organization must also provide the Department with a copy of its human resources privacy policy and provide information where the privacy policy is available for viewing by its affected employees.
- d. The Department will maintain the Privacy Shield List of organizations that file completed self-certification submissions, thereby assuring the

Decision and Order

- availability of Privacy Shield benefits, and will update such list on the basis of annual self-recertification submissions and notifications received pursuant to the Supplemental Principle on Dispute Resolution and Enforcement. Such self-certification submissions must be provided not less than annually; otherwise the organization will be removed from the Privacy Shield List and Privacy Shield benefits will no longer be assured. Both the Privacy Shield List and the self-certification submissions by the organizations will be made publicly available. All organizations that are placed on the Privacy Shield List by the Department must also state in their relevant published privacy policy statements that they adhere to the Privacy Shield Principles. If available online, an organization's privacy policy must include a hyperlink to the Department's Privacy Shield website and a hyperlink to the website or complaint submission form of the independent recourse mechanism that is available to investigate unresolved complaints.
- e. The Privacy Principles apply immediately upon certification. Recognizing that the Principles will impact commercial relationships with third parties, organizations that certify to the Privacy Shield Framework in the first two months following the Framework's effective date shall bring existing commercial relationships with third parties into conformity with the Accountability for Onward Transfer Principle as soon as possible, and in any event no later than nine months from the date upon which they certify to the Privacy Shield. During that interim period, where organizations transfer data to a third party, they shall (i) apply the Notice and Choice Principles, and (ii) where personal data is transferred to a third party acting as an agent, ascertain that the agent is obligated to provide at least the same level of protection as is required by the Principles.
 - f. An organization must subject to the Privacy Shield Principles all personal data received from the EU in reliance upon the Privacy Shield. The undertaking to adhere to the Privacy Shield Principles is not time-limited in respect of personal data received during the period in which the organization enjoys the benefits of the Privacy Shield. Its undertaking means that it will continue to apply the Principles to such data for as long as the organization stores, uses or discloses them, even if it subsequently leaves the Privacy Shield for any reason. An organization that withdraws from the Privacy Shield but wants to retain such data must affirm to the Department on an annual basis its commitment to continue to apply the Principles or provide "adequate" protection for the information by another authorized means (for example, using a contract that fully reflects the requirements of the relevant standard contractual clauses adopted by the European Commission); otherwise, the organization must return or delete the information. An organization that withdraws from the Privacy Shield must remove from any relevant privacy policy any references to the Privacy Shield that imply that the organization continues to actively participate in the Privacy Shield and is entitled to its benefits.

Decision and Order

- g. An organization that will cease to exist as a separate legal entity as a result of a merger or a takeover must notify the Department of this in advance. The notification should also indicate whether the acquiring entity or the entity resulting from the merger will (i) continue to be bound by the Privacy Shield Principles by the operation of law governing the takeover or merger or (ii) elect to self-certify its adherence to the Privacy Shield Principles or put in place other safeguards, such as a written agreement that will ensure adherence to the Privacy Shield Principles. Where neither (i) nor (ii) applies, any personal data that has been acquired under the Privacy Shield must be promptly deleted.
- h. When an organization leaves the Privacy Shield for any reason, it must remove all statements implying that the organization continues to participate in the Privacy Shield or is entitled to the benefits of the Privacy Shield. The EU-U.S. Privacy Shield certification mark, if used, must also be removed. Any misrepresentation to the general public concerning an organization's adherence to the Privacy Shield Principles may be actionable by the FTC or other relevant government body. Misrepresentations to the Department may be actionable under the False Statements Act (18 U.S.C. § 1001).

7. Verification

- a. Organizations must provide follow up procedures for verifying that the attestations and assertions they make about their Privacy Shield privacy practices are true and those privacy practices have been implemented as represented and in accordance with the Privacy Shield Principles.
- b. To meet the verification requirements of the Recourse, Enforcement and Liability Principle, an organization must verify such attestations and assertions either through self-assessment or outside compliance reviews.
- c. Under the self-assessment approach, such verification must indicate that an organization's published privacy policy regarding personal information received from the EU is accurate, comprehensive, prominently displayed, completely implemented and accessible. It must also indicate that its privacy policy conforms to the Privacy Shield Principles; that individuals are informed of any in-house arrangements for handling complaints and of the independent mechanisms through which they may pursue complaints; that it has in place procedures for training employees in its implementation, and disciplining them for failure to follow it; and that it has in place internal procedures for periodically conducting objective reviews of compliance with the above. A statement verifying the self-assessment must be signed by a corporate officer or other authorized representative of the organization at least once a year and made available upon request by individuals or in the context of an investigation or a complaint about non-compliance.
- d. Where the organization has chosen outside compliance review, such a review must demonstrate that its privacy policy regarding personal

Decision and Order

information received from the EU conforms to the Privacy Shield Principles, that it is being complied with, and that individuals are informed of the mechanisms through which they may pursue complaints. The methods of review may include, without limitation, auditing, random reviews, use of “decoys”, or use of technology tools as appropriate. A statement verifying that an outside compliance review has been successfully completed must be signed either by the reviewer or by the corporate officer or other authorized representative of the organization at least once a year and made available upon request by individuals or in the context of an investigation or a complaint about compliance.

- e. Organizations must retain their records on the implementation of their Privacy Shield privacy practices and make them available upon request in the context of an investigation or a complaint about non-compliance to the independent body responsible for investigating complaints or to the agency with unfair and deceptive practices jurisdiction. Organizations must also respond promptly to inquiries and other requests for information from the Department relating to the organization’s adherence to the Principles.

8. Access

a. The Access Principle in Practice

- i. Under the Privacy Shield Principles, the right of access is fundamental to privacy protection. In particular, it allows individuals to verify the accuracy of information held about them. The Access Principle means that individuals have the right to:
 - 1. obtain from an organization confirmation of whether or not the organization is processing personal data relating to them;⁴
 - 2. have communicated to them such data so that they could verify its accuracy and the lawfulness of the processing; and
 - 3. have the data corrected, amended or deleted where it is inaccurate or processed in violation of the Principles.
- ii. Individuals do not have to justify requests for access to their personal data. In responding to individuals’ access requests, organizations should first be guided by the concern(s) that led to the requests in the first place. For example, if an access request is vague or broad in scope, an organization may engage the individual in a dialogue so as to better understand the motivation for the request and to locate responsive information. The organization might

⁴ The organization should answer requests from an individual concerning the purposes of the processing, the categories of personal data concerned, and the recipients or categories of recipients to whom the personal data is disclosed.

Decision and Order

inquire about which part(s) of the organization the individual interacted with or about the nature of the information or its use that is the subject of the access request.

- iii. Consistent with the fundamental nature of access, organizations should always make good faith efforts to provide access. For example, where certain information needs to be protected and can be readily separated from other personal information subject to an access request, the organization should redact the protected information and make available the other information. If an organization determines that access should be restricted in any particular instance, it should provide the individual requesting access with an explanation of why it has made that determination and a contact point for any further inquiries.

b. Burden or Expense of Providing Access

- i. The right of access to personal data may be restricted in exceptional circumstances where the legitimate rights of persons other than the individual would be violated or where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question. Expense and burden are important factors and should be taken into account but they are not controlling factors in determining whether providing access is reasonable.
- ii. For example, if the personal information is used for decisions that will significantly affect the individual (*e.g.*, the denial or grant of important benefits, such as insurance, a mortgage, or a job), then consistent with the other provisions of these Supplemental Principles, the organization would have to disclose that information even if it is relatively difficult or expensive to provide. If the personal information requested is not sensitive or not used for decisions that will significantly affect the individual, but is readily available and inexpensive to provide, an organization would have to provide access to such information.

c. Confidential Commercial Information

- i. Confidential commercial information is information that an organization has taken steps to protect from disclosure, where disclosure would help a competitor in the market. Organizations may deny or limit access to the extent that granting full access would reveal its own confidential commercial information, such as marketing inferences or classifications generated by the organization, or the confidential commercial information of another that is subject to a contractual obligation of confidentiality.

Decision and Order

- ii. Where confidential commercial information can be readily separated from other personal information subject to an access request, the organization should redact the confidential commercial information and make available the non-confidential information.
- d. Organization of Data Bases
 - i. Access can be provided in the form of disclosure of the relevant personal information by an organization to the individual and does not require access by the individual to an organization's data base.
 - ii. Access needs to be provided only to the extent that an organization stores the personal information. The Access Principle does not itself create any obligation to retain, maintain, reorganize, or restructure personal information files.
- e. When Access May be Restricted
 - i. As organizations must always make good faith efforts to provide individuals with access to their personal data, the circumstances in which organizations may restrict such access are limited, and any reasons for restricting access must be specific. As under the Directive, an organization can restrict access to information to the extent that disclosure is likely to interfere with the safeguarding of important countervailing public interests, such as national security, defense, or public security. In addition, where personal information is processed solely for research or statistical purposes, access may be denied. Other reasons for denying or limiting access are:
 - 1. interference with the execution or enforcement of the law or with private causes of action, including the prevention, investigation or detection of offenses or the right to a fair trial;
 - 2. disclosure where the legitimate rights or important interests of others would be violated;
 - 3. breaching a legal or other professional privilege or obligation;
 - 4. prejudicing employee security investigations or grievance proceedings or in connection with employee succession planning and corporate re-organizations; or
 - 5. prejudicing the confidentiality necessary in monitoring, inspection or regulatory functions connected with sound management, or in future or ongoing negotiations involving the organization.
 - ii. An organization which claims an exception has the burden of demonstrating its necessity, and the reasons for restricting access

Decision and Order

and a contact point for further inquiries should be given to individuals.

- f. Right to Obtain Confirmation and Charging a Fee to Cover the Costs for Providing Access
 - i. An individual has the right to obtain confirmation of whether or not this organization has personal data relating to him or her. An individual also has the right to have communicated to him or her personal data relating to him or her. An organization may charge a fee that is not excessive.
 - ii. Charging a fee may be justified, for example, where requests for access are manifestly excessive, in particular because of their repetitive character.
 - iii. Access may not be refused on cost grounds if the individual offers to pay the costs.
- g. Repetitious or Vexatious Requests for Access
 - i. An organization may set reasonable limits on the number of times within a given period that access requests from a particular individual will be met. In setting such limitations, an organization should consider such factors as the frequency with which information is updated, the purpose for which the data are used, and the nature of the information.
- h. Fraudulent Requests for Access
 - i. An organization is not required to provide access unless it is supplied with sufficient information to allow it to confirm the identity of the person making the request.
- i. Timeframe for Responses
 - i. Organizations should respond to access requests within a reasonable time period, in a reasonable manner, and in a form that is readily intelligible to the individual. An organization that provides information to data subjects at regular intervals may satisfy an individual access request with its regular disclosure if it would not constitute an excessive delay.

9. **Human Resources Data**

- a. Coverage by the Privacy Shield
 - i. Where an organization in the EU transfers personal information about its employees (past or present) collected in the context of the employment relationship, to a parent, affiliate, or unaffiliated service provider in the United States participating in the Privacy Shield, the transfer enjoys the benefits of the Privacy Shield. In

Decision and Order

such cases, the collection of the information and its processing prior to transfer will have been subject to the national laws of the EU country where it was collected, and any conditions for or restrictions on its transfer according to those laws will have to be respected.

- ii. The Privacy Shield Principles are relevant only when individually identified or identifiable records are transferred or accessed. Statistical reporting relying on aggregate employment data and containing no personal data or the use of anonymized data does not raise privacy concerns.

b. Application of the Notice and Choice Principles

- i. A U.S. organization that has received employee information from the EU under the Privacy Shield may disclose it to third parties or use it for different purposes only in accordance with the Notice and Choice Principles. For example, where an organization intends to use personal information collected through the employment relationship for non-employment-related purposes, such as marketing communications, the U.S. organization must provide the affected individuals with the requisite choice before doing so, unless they have already authorized the use of the information for such purposes. Such use must not be incompatible with the purposes for which the personal information has been collected or subsequently authorized by the individual. Moreover, such choices must not be used to restrict employment opportunities or take any punitive action against such employees.
- ii. It should be noted that certain generally applicable conditions for transfer from some EU Member States may preclude other uses of such information even after transfer outside the EU and such conditions will have to be respected.
- iii. In addition, employers should make reasonable efforts to accommodate employee privacy preferences. This could include, for example, restricting access to the personal data, anonymizing certain data, or assigning codes or pseudonyms when the actual names are not required for the management purpose at hand.
- iv. To the extent and for the period necessary to avoid prejudicing the ability of the organization in making promotions, appointments, or other similar employment decisions, an organization does not need to offer notice and choice.

c. Application of the Access Principle

- i. The Supplemental Principle on Access provides guidance on reasons which may justify denying or limiting access on request in the human resources context. Of course, employers in the European Union must comply with local regulations and ensure that European

Decision and Order

Union employees have access to such information as is required by law in their home countries, regardless of the location of data processing and storage. The Privacy Shield requires that an organization processing such data in the United States will cooperate in providing such access either directly or through the EU employer.

d. Enforcement

- i. In so far as personal information is used only in the context of the employment relationship, primary responsibility for the data vis-à-vis the employee remains with the organization in the EU. It follows that, where European employees make complaints about violations of their data protection rights and are not satisfied with the results of internal review, complaint, and appeal procedures (or any applicable grievance procedures under a contract with a trade union), they should be directed to the state or national data protection or labor authority in the jurisdiction where the employees work. This includes cases where the alleged mishandling of their personal information is the responsibility of the U.S. organization that has received the information from the employer and thus involves an alleged breach of the Privacy Shield Principles. This will be the most efficient way to address the often overlapping rights and obligations imposed by local labor law and labor agreements as well as data protection law.
- ii. A U.S. organization participating in the Privacy Shield that uses EU human resources data transferred from the European Union in the context of the employment relationship and that wishes such transfers to be covered by the Privacy Shield must therefore commit to cooperate in investigations by and to comply with the advice of competent EU authorities in such cases.

e. Application of the Accountability for Onward Transfer Principle

- i. For occasional employment-related operational needs of the Privacy Shield organization with respect to personal data transferred under the Privacy Shield, such as the booking of a flight, hotel room, or insurance coverage, transfers of personal data of a small number of employees can take place to controllers without application of the Access Principle or entering into a contract with the third-party controller, as otherwise required under the Accountability for Onward Transfer Principle, provided that the Privacy Shield organization has complied with the Notice and Choice Principles.

10. **Obligatory Contracts for Onward Transfers**

a. Data Processing Contracts

Decision and Order

- i. When personal data is transferred from the EU to the United States only for processing purposes, a contract will be required, regardless of participation by the processor in the Privacy Shield.
 - ii. Data controllers in the European Union are always required to enter into a contract when a transfer for mere processing is made, whether the processing operation is carried out inside or outside the EU, and whether or not the processor participates in the Privacy Shield. The purpose of the contract is to make sure that the processor:
 - 1. acts only on instructions from the controller;
 - 2. provides appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and understands whether onward transfer is allowed; and
 - 3. taking into account the nature of the processing, assists the controller in responding to individuals exercising their rights under the Principles.
 - iii. Because adequate protection is provided by Privacy Shield participants, contracts with Privacy Shield participants for mere processing do not require prior authorization (or such authorization will be granted automatically by the EU Member States), as would be required for contracts with recipients not participating in the Privacy Shield or otherwise not providing adequate protection.
- b. Transfers within a Controlled Group of Corporations or Entities
- i. When personal information is transferred between two controllers within a controlled group of corporations or entities, a contract is not always required under the Accountability for Onward Transfer Principle. Data controllers within a controlled group of corporations or entities may base such transfers on other instruments, such as EU Binding Corporate Rules or other intra-group instruments (e.g., compliance and control programs), ensuring the continuity of protection of personal information under the Principles. In case of such transfers, the Privacy Shield organization remains responsible for compliance with the Principles.
- c. Transfers between Controllers
- i. For transfers between controllers, the recipient controller need not be a Privacy Shield organization or have an independent recourse mechanism. The Privacy Shield organization must enter into a contract with the recipient third-party controller that provides for the same level of protection as is available under the Privacy Shield,

Decision and Order

not including the requirement that the third party controller be a Privacy Shield organization or have an independent recourse mechanism, provided it makes available an equivalent mechanism.

11. Dispute Resolution and Enforcement

- a. The Recourse, Enforcement and Liability Principle sets out the requirements for Privacy Shield enforcement. How to meet the requirements of point (a)(ii) of the Principle is set out in the Supplemental Principle on Verification. This Supplemental Principle addresses points (a)(i) and (a)(iii), both of which require independent recourse mechanisms. These mechanisms may take different forms, but they must meet the Recourse, Enforcement and Liability Principle's requirements. Organizations satisfy the requirements through the following: (i) compliance with private sector developed privacy programs that incorporate the Privacy Shield Principles into their rules and that include effective enforcement mechanisms of the type described in the Recourse, Enforcement and Liability Principle; (ii) compliance with legal or regulatory supervisory authorities that provide for handling of individual complaints and dispute resolution; or (iii) commitment to cooperate with data protection authorities located in the European Union or their authorized representatives.
- b. This list is intended to be illustrative and not limiting. The private sector may design additional mechanisms to provide enforcement, so long as they meet the requirements of the Recourse, Enforcement and Liability Principle and the Supplemental Principles. Please note that the Recourse, Enforcement and Liability Principle's requirements are additional to the requirement that self-regulatory efforts must be enforceable under Section 5 of the Federal Trade Commission Act, which prohibits unfair and deceptive acts, or another law or regulation prohibiting such acts.
- c. In order to help ensure compliance with their Privacy Shield commitments and to support the administration of the program, organizations, as well as their independent recourse mechanisms, must provide information relating to the Privacy Shield when requested by the Department. In addition, organizations must respond expeditiously to complaints regarding their compliance with the Principles referred through the Department by DPAs. The response should address whether the complaint has merit and, if so, how the organization will rectify the problem. The Department will protect the confidentiality of information it receives in accordance with U.S. law.
- d. Recourse Mechanisms
 - i. Consumers should be encouraged to raise any complaints they may have with the relevant organization before proceeding to independent recourse mechanisms. Organizations must respond to a consumer within 45 days of receiving a complaint. Whether a recourse mechanism is independent is a factual question that can be

Decision and Order

demonstrated notably by impartiality, transparent composition and financing, and a proven track record. As required by the Recourse, Enforcement and Liability Principle, the recourse available to individuals must be readily available and free of charge to individuals. Dispute resolution bodies should look into each complaint received from individuals unless they are obviously unfounded or frivolous. This does not preclude the establishment of eligibility requirements by the organization operating the recourse mechanism, but such requirements should be transparent and justified (for example, to exclude complaints that fall outside the scope of the program or are for consideration in another forum), and should not have the effect of undermining the commitment to look into legitimate complaints. In addition, recourse mechanisms should provide individuals with full and readily available information about how the dispute resolution procedure works when they file a complaint. Such information should include notice about the mechanism's privacy practices, in conformity with the Privacy Shield Principles. They should also cooperate in the development of tools such as standard complaint forms to facilitate the complaint resolution process.

- ii. Independent recourse mechanisms must include on their public websites information regarding the Privacy Shield Principles and the services that they provide under the Privacy Shield. This information must include: (1) information on or a link to the Privacy Shield Principles' requirements for independent recourse mechanisms; (2) a link to the Department's Privacy Shield website; (3) an explanation that their dispute resolution services under the Privacy Shield are free of charge to individuals; (4) a description of how a Privacy Shield-related complaint can be filed; (5) the timeframe in which Privacy Shield-related complaints are processed; and (6) a description of the range of potential remedies.
- iii. Independent recourse mechanisms must publish an annual report providing aggregate statistics regarding their dispute resolution services. The annual report must include: (1) the total number of Privacy Shield-related complaints received during the reporting year; (2) the types of complaints received; (3) dispute resolution quality measures, such as the length of time taken to process complaints; and (4) the outcomes of the complaints received, notably the number and types of remedies or sanctions imposed.
- iv. As set forth in Annex I, an arbitration option is available to an individual to determine, for residual claims, whether a Privacy Shield organization has violated its obligations under the Principles as to that individual, and whether any such violation remains fully or partially unremedied. This option is available only for these purposes. This option is not available, for example, with respect to

Decision and Order

the exceptions to the Principles⁵ or with respect to an allegation about the adequacy of the Privacy Shield. Under this arbitration option, the Privacy Shield Panel (consisting of one or three arbitrators, as agreed by the parties) has the authority to impose individual-specific, non-monetary equitable relief (such as access, correction, deletion, or return of the individual's data in question) necessary to remedy the violation of the Principles only with respect to the individual. Individuals and Privacy Shield organizations will be able to seek judicial review and enforcement of the arbitral decisions pursuant to U.S. law under the Federal Arbitration Act.

e. Remedies and Sanctions

- i. The result of any remedies provided by the dispute resolution body should be that the effects of non-compliance are reversed or corrected by the organization, insofar as feasible, and that future processing by the organization will be in conformity with the Principles and, where appropriate, that processing of the personal data of the individual who brought the complaint will cease. Sanctions need to be rigorous enough to ensure compliance by the organization with the Principles. A range of sanctions of varying degrees of severity will allow dispute resolution bodies to respond appropriately to varying degrees of non-compliance. Sanctions should include both publicity for findings of non-compliance and the requirement to delete data in certain circumstances.⁶ Other sanctions could include suspension and removal of a seal, compensation for individuals for losses incurred as a result of non-compliance and injunctive awards. Private sector dispute resolution bodies and self-regulatory bodies must notify failures of Privacy Shield organizations to comply with their rulings to the governmental body with applicable jurisdiction or to the courts, as appropriate, and to notify the Department.

f. FTC Action

- ii. The FTC has committed to reviewing on a priority basis referrals alleging non-compliance with the Principles received from: (i) privacy self-regulatory organizations and other independent dispute resolution bodies; (ii) EU Member States; and (iii) the Department, to determine whether Section 5 of the FTC Act prohibiting unfair or deceptive acts or practices in commerce has been violated. If the FTC concludes that it has reason to believe Section 5 has been

⁵ Section I.5 of the Principles.

⁶ Dispute resolution bodies have discretion about the circumstances in which they use these sanctions. The sensitivity of the data concerned is one factor to be taken into consideration in deciding whether deletion of data should be required, as is whether an organization has collected, used, or disclosed information in blatant contravention of the Privacy Shield Principles.

Decision and Order

violated, it may resolve the matter by seeking an administrative cease and desist order prohibiting the challenged practices or by filing a complaint in a federal district court, which if successful could result in a federal court order to same effect. This includes false claims of adherence to the Privacy Shield Principles or participation in the Privacy Shield by organizations, which either are no longer on the Privacy Shield List or have never self-certified to the Department. The FTC may obtain civil penalties for violations of an administrative cease and desist order and may pursue civil or criminal contempt for violation of a federal court order. The FTC will notify the Department of any such actions it takes. The Department encourages other government bodies to notify it of the final disposition of any such referrals or other rulings determining adherence to the Privacy Shield Principles.

g. Persistent Failure to Comply

- i. If an organization persistently fails to comply with the Principles, it is no longer entitled to benefit from the Privacy Shield. Organizations that have persistently failed to comply with the Principles will be removed from the Privacy Shield List by the Department and must return or delete the personal information they received under the Privacy Shield.
- ii. Persistent failure to comply arises where an organization that has self-certified to the Department refuses to comply with a final determination by any privacy self-regulatory, independent dispute resolution, or government body, or where such a body determines that an organization frequently fails to comply with the Principles to the point where its claim to comply is no longer credible. In these cases, the organization must promptly notify the Department of such facts. Failure to do so may be actionable under the False Statements Act (18 U.S.C. § 1001). An organization's withdrawal from a private-sector privacy self-regulatory program or independent dispute resolution mechanism does not relieve it of its obligation to comply with the Principles and would constitute a persistent failure to comply.
- iii. The Department will remove an organization from the Privacy Shield List in response to any notification it receives of persistent failure to comply, whether it is received from the organization itself, from a privacy self-regulatory body or another independent dispute resolution body, or from a government body, but only after first providing 30 days' notice and an opportunity to respond to the organization that has failed to comply. Accordingly, the Privacy Shield List maintained by the Department will make clear which organizations are assured and which organizations are no longer assured of Privacy Shield benefits.

Decision and Order

- iv. An organization applying to participate in a self-regulatory body for the purposes of requalifying for the Privacy Shield must provide that body with full information about its prior participation in the Privacy Shield.

12. Choice – Timing of Opt Out

- a. Generally, the purpose of the Choice Principle is to ensure that personal information is used and disclosed in ways that are consistent with the individual's expectations and choices. Accordingly, an individual should be able to exercise "opt out" choice of having personal information used for direct marketing at any time subject to reasonable limits established by the organization, such as giving the organization time to make the opt out effective. An organization may also require sufficient information to confirm the identity of the individual requesting the "opt out." In the United States, individuals may be able to exercise this option through the use of a central "opt out" program such as the Direct Marketing Association's Mail Preference Service. Organizations that participate in the Direct Marketing Association's Mail Preference Service should promote its availability to consumers who do not wish to receive commercial information. In any event, an individual should be given a readily available and affordable mechanism to exercise this option.
- b. Similarly, an organization may use information for certain direct marketing purposes when it is impracticable to provide the individual with an opportunity to opt out before using the information, if the organization promptly gives the individual such opportunity at the same time (and upon request at any time) to decline (at no cost to the individual) to receive any further direct marketing communications and the organization complies with the individual's wishes.

13. Travel Information

- a. Airline passenger reservation and other travel information, such as frequent flyer or hotel reservation information and special handling needs, such as meals to meet religious requirements or physical assistance, may be transferred to organizations located outside the EU in several different circumstances. Under Article 26 of the Directive, personal data may be transferred "to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2)" on the condition that it (i) is necessary to provide the services requested by the consumer or to fulfill the terms of an agreement, such as a "frequent flyer" agreement; or (ii) has been unambiguously consented to by the consumer. U.S. organizations subscribing to the Privacy Shield provide adequate protection for personal data and may therefore receive data transfers from the EU without meeting these conditions or other conditions set out in Article 26 of the Directive. Since the Privacy Shield includes specific rules for sensitive information, such information (which may need to be collected, for example, in

Decision and Order

connection with customers' needs for physical assistance) may be included in transfers to Privacy Shield participants. In all cases, however, the organization transferring the information has to respect the law in the EU Member State in which it is operating, which may inter alia impose special conditions for the handling of sensitive data.

14. Pharmaceutical and Medical Products

- a. Application of EU Member State Laws or the Privacy Shield Principles
 - i. EU Member State law applies to the collection of the personal data and to any processing that takes place prior to the transfer to the United States. The Privacy Shield Principles apply to the data once they have been transferred to the United States. Data used for pharmaceutical research and other purposes should be anonymized when appropriate.
- b. Future Scientific Research
 - i. Personal data developed in specific medical or pharmaceutical research studies often play a valuable role in future scientific research. Where personal data collected for one research study are transferred to a U.S. organization in the Privacy Shield, the organization may use the data for a new scientific research activity if appropriate notice and choice have been provided in the first instance. Such notice should provide information about any future specific uses of the data, such as periodic follow-up, related studies, or marketing.
 - ii. It is understood that not all future uses of the data can be specified, since a new research use could arise from new insights on the original data, new medical discoveries and advances, and public health and regulatory developments. Where appropriate, the notice should therefore include an explanation that personal data may be used in future medical and pharmaceutical research activities that are unanticipated. If the use is not consistent with the general research purpose(s) for which the personal data were originally collected, or to which the individual has consented subsequently, new consent must be obtained.
- c. Withdrawal from a Clinical Trial
 - i. Participants may decide or be asked to withdraw from a clinical trial at any time. Any personal data collected previous to withdrawal may still be processed along with other data collected as part of the clinical trial, however, if this was made clear to the participant in the notice at the time he or she agreed to participate.
- d. Transfers for Regulatory and Supervision Purposes

Decision and Order

- i. Pharmaceutical and medical device companies are allowed to provide personal data from clinical trials conducted in the EU to regulators in the United States for regulatory and supervision purposes. Similar transfers are allowed to parties other than regulators, such as company locations and other researchers, consistent with the Principles of Notice and Choice.
- e. “Blinded” Studies
 - i. To ensure objectivity in many clinical trials, participants, and often investigators as well, cannot be given access to information about which treatment each participant may be receiving. Doing so would jeopardize the validity of the research study and results. Participants in such clinical trials (referred to as “blinded” studies) do not have to be provided access to the data on their treatment during the trial if this restriction has been explained when the participant entered the trial and the disclosure of such information would jeopardize the integrity of the research effort.
 - ii. Agreement to participate in the trial under these conditions is a reasonable forgoing of the right of access. Following the conclusion of the trial and analysis of the results, participants should have access to their data if they request it. They should seek it primarily from the physician or other health care provider from whom they received treatment within the clinical trial, or secondarily from the sponsoring organization.
- f. Product Safety and Efficacy Monitoring
 - i. A pharmaceutical or medical device company does not have to apply the Privacy Shield Principles with respect to the Notice, Choice, Accountability for Onward Transfer, and Access Principles in its product safety and efficacy monitoring activities, including the reporting of adverse events and the tracking of patients/subjects using certain medicines or medical devices, to the extent that adherence to the Principles interferes with compliance with regulatory requirements. This is true both with respect to reports by, for example, health care providers to pharmaceutical and medical device companies, and with respect to reports by pharmaceutical and medical device companies to government agencies like the Food and Drug Administration.
- g. Key-coded Data
 - i. Invariably, research data are uniquely key-coded at their origin by the principal investigator so as not to reveal the identity of individual data subjects. Pharmaceutical companies sponsoring such research do not receive the key. The unique key code is held only by the researcher, so that he or she can identify the research subject under special circumstances (e.g., if follow-up medical attention is

Decision and Order

required). A transfer from the EU to the United States of data coded in this way would not constitute a transfer of personal data that would be subject to the Privacy Shield Principles.

15. Public Record and Publicly Available Information

- a. An organization must apply the Privacy Shield Principles of Security, Data Integrity and Purpose Limitation, and Recourse, Enforcement and Liability to personal data from publicly available sources. These Principles shall apply also to personal data collected from public records, *i.e.*, those records kept by government agencies or entities at any level that are open to consultation by the public in general.
- b. It is not necessary to apply the Notice, Choice, or Accountability for Onward Transfer Principles to public record information, as long as it is not combined with non-public record information, and any conditions for consultation established by the relevant jurisdiction are respected. Also, it is generally not necessary to apply the Notice, Choice, or Accountability for Onward Transfer Principles to publicly available information unless the European transferor indicates that such information is subject to restrictions that require application of those Principles by the organization for the uses it intends. Organizations will have no liability for how such information is used by those obtaining such information from published materials.
- c. Where an organization is found to have intentionally made personal information public in contravention of the Principles so that it or others may benefit from these exceptions, it will cease to qualify for the benefits of the Privacy Shield.
- d. It is not necessary to apply the Access Principle to public record information as long as it is not combined with other personal information (apart from small amounts used to index or organize the public record information); however, any conditions for consultation established by the relevant jurisdiction are to be respected. In contrast, where public record information is combined with other non-public record information (other than as specifically noted above), an organization must provide access to all such information, assuming it is not subject to other permitted exceptions.
- e. As with public record information, it is not necessary to provide access to information that is already publicly available to the public at large, as long as it is not combined with non-publicly available information. Organizations that are in the business of selling publicly available information may charge the organization's customary fee in responding to requests for access. Alternatively, individuals may seek access to their information from the organization that originally compiled the data.

16. Access Requests by Public Authorities

Decision and Order

- a. In order to provide transparency in respect of lawful requests by public authorities to access personal information, Privacy Shield organizations may voluntarily issue periodic transparency reports on the number of requests for personal information they receive by public authorities for law enforcement or national security reasons, to the extent such disclosures are permissible under applicable law.
- b. The information provided by the Privacy Shield organizations in these reports together with information that has been released by the intelligence community, along with other information, can be used to inform the annual joint review of the functioning of the Privacy Shield in accordance with the Principles.
- c. Absence of notice in accordance with point (a)(xii) of the Notice Principle shall not prevent or impair an organization's ability to respond to any lawful request.

Decision and Order

ANNEX I: Arbitral Model

Decision and Order

ANNEX I

This Annex I provides the terms under which Privacy Shield organizations are obligated to arbitrate claims, pursuant to the Recourse, Enforcement and Liability Principle. The binding arbitration option described below applies to certain “residual” claims as to data covered by the EU-U.S. Privacy Shield. The purpose of this option is to provide a prompt, independent, and fair mechanism, at the option of individuals, for resolution of claimed violations of the Principles not resolved by any of the other Privacy Shield mechanisms, if any.

A. Scope

This arbitration option is available to an individual to determine, for residual claims, whether a Privacy Shield organization has violated its obligations under the Principles as to that individual, and whether any such violation remains fully or partially unremedied. This option is available only for these purposes. This option is not available, for example, with respect to the exceptions to the Principles¹ or with respect to an allegation about the adequacy of the Privacy Shield.

B. Available Remedies

Under this arbitration option, the Privacy Shield Panel (consisting of one or three arbitrators, as agreed by the parties) has the authority to impose individual-specific, non-monetary equitable relief (such as access, correction, deletion, or return of the individual’s data in question) necessary to remedy the violation of the Principles only with respect to the individual. These are the only powers of the arbitration panel with respect to remedies. In considering remedies, the arbitration panel is required to consider other remedies that already have been imposed by other mechanisms under the Privacy Shield. No damages, costs, fees, or other remedies are available. Each party bears its own attorney’s fees.

C. Pre-Arbitration Requirements

An individual who decides to invoke this arbitration option must take the following steps prior to initiating an arbitration claim: (1) raise the claimed violation directly with the organization and afford the organization an opportunity to resolve the issue within the timeframe set forth in Section III.11(d)(i) of the Principles; (2) make use of the independent recourse mechanism under the Principles, which is at no cost to the individual; and (3) raise the issue through their Data Protection Authority to the Department of Commerce and afford the Department of Commerce an opportunity to use best efforts to resolve the issue within the timeframes set forth in the Letter from the International Trade Administration of the Department of Commerce, at no cost to the individual.

This arbitration option may not be invoked if the individual’s same claimed violation of the Principles (1) has previously been subject to binding arbitration; (2) was the subject of a final judgment entered in a court action to which the individual was a party; or (3) was previously settled by the parties. In addition, this option may not be invoked if an EU Data Protection

¹ Section I.5 of the Principles.

Decision and Order

Authority (1) has authority under Sections III.5 or III.9 of the Principles; or (2) has the authority to resolve the claimed violation directly with the organization. A DPA's authority to resolve the same claim against an EU data controller does not alone preclude invocation of this arbitration option against a different legal entity not bound by the DPA authority.

D. Binding Nature of Decisions

An individual's decision to invoke this binding arbitration option is entirely voluntary. Arbitral decisions will be binding on all parties to the arbitration. Once invoked, the individual forgoes the option to seek relief for the same claimed violation in another forum, except that if non-monetary equitable relief does not fully remedy the claimed violation, the individual's invocation of arbitration will not preclude a claim for damages that is otherwise available in the courts.

E. Review and Enforcement

Individuals and Privacy Shield organizations will be able to seek judicial review and enforcement of the arbitral decisions pursuant to U.S. law under the Federal Arbitration Act.² Any such cases must be brought in the federal district court whose territorial coverage includes the primary place of business of the Privacy Shield organization.

²Chapter 2 of the Federal Arbitration Act ("FAA") provides that "[a]n arbitration agreement or arbitral award arising out of a legal relationship, whether contractual or not, which is considered as commercial, including a transaction, contract, or agreement described in [section 2 of the FAA], falls under the Convention [on the Recognition and Enforcement of Foreign Arbitral Awards of June 10, 1958, 21 U.S.T. 2519, T.I.A.S. No. 6997 ("New York Convention")." 9 U.S.C. § 202. The FAA further provides that "[a]n agreement or award arising out of such a relationship which is entirely between citizens of the United States shall be deemed not to fall under the [New York] Convention unless that relationship involves property located abroad, envisages performance or enforcement abroad, or has some other reasonable relation with one or more foreign states." *Id.* Under Chapter 2, "any party to the arbitration may apply to any court having jurisdiction under this chapter for an order confirming the award as against any other party to the arbitration. The court shall confirm the award unless it finds one of the grounds for refusal or deferral of recognition or enforcement of the award specified in the said [New York] Convention." *Id.* § 207. Chapter 2 further provides that "[t]he district courts of the United States . . . shall have original jurisdiction over . . . an action or proceeding [under the New York Convention], regardless of the amount in controversy." *Id.* § 203.

Chapter 2 also provides that "Chapter 1 applies to actions and proceedings brought under this chapter to the extent that chapter is not in conflict with this chapter or the [New York] Convention as ratified by the United States." *Id.* § 208. Chapter 1, in turn, provides that "[a] written provision in . . . a contract evidencing a transaction involving commerce to settle by arbitration a controversy thereafter arising out of such contract or transaction, or the refusal to perform the whole or any part thereof, or an agreement in writing to submit to arbitration an existing controversy arising out of such a contract, transaction, or refusal, shall be valid, irrevocable, and enforceable, save upon such grounds as exist at law or in equity for the revocation of any contract." *Id.* § 2. Chapter 1 further provides that "any party to the arbitration may apply to the court so specified for an order confirming the award, and thereupon the court must grant such an order unless the award is vacated, modified, or corrected as prescribed in sections 10 and 11 of [the FAA]." *Id.* § 9.

Decision and Order

This arbitration option is intended to resolve individual disputes, and arbitral decisions are not intended to function as persuasive or binding precedent in matters involving other parties, including in future arbitrations or in EU or U.S. courts, or FTC proceedings.

F. The Arbitration Panel

The parties will select the arbitrators from the list of arbitrators discussed below.

Consistent with applicable law, the U.S. Department of Commerce and the European Commission will develop a list of at least 20 arbitrators, chosen on the basis of independence, integrity, and expertise. The following shall apply in connection with this process:

Arbitrators:

- (1) will remain on the list for a period of 3 years, absent exceptional circumstances or for cause, renewable for one additional period of 3 years;
- (2) shall not be subject to any instructions from, or be affiliated with, either party, or any Privacy Shield organization, or the U.S., EU, or any EU Member State or any other governmental authority, public authority, or enforcement authority; and
- (3) must be admitted to practice law in the U.S. and be experts in U.S. privacy law, with expertise in EU data protection law.

G. Arbitration Procedures

Consistent with applicable law, within 6 months from the adoption of the adequacy decision, the Department of Commerce and the European Commission will agree to adopt an existing, well-established set of U.S. arbitral procedures (such as AAA or JAMS) to govern proceedings before the Privacy Shield Panel, subject to each of the following considerations:

1. An individual may initiate binding arbitration, subject to the pre-arbitration requirements provision above, by delivering a "Notice" to the organization. The Notice shall contain a summary of steps taken under Paragraph C to resolve the claim, a description of the alleged violation, and, at the choice of the individual, any supporting documents and materials and/or a discussion of law relating to the alleged claim.
2. Procedures will be developed to ensure that an individual's same claimed violation does not receive duplicative remedies or procedures.
3. FTC action may proceed in parallel with arbitration.
4. No representative of the U.S., EU, or any EU Member State or any other governmental authority, public authority, or enforcement authority may participate in these arbitrations, provided, that at the request of an EU individual, EU DPAs may provide assistance in the preparation only of the Notice but EU DPAs may not have access to discovery or any other materials related to these arbitrations.
5. The location of the arbitration will be the United States, and the individual may choose video or telephone participation, which will be provided at no cost to the individual. In-person participation will not be required.

Decision and Order

6. The language of the arbitration will be English unless otherwise agreed by the parties. Upon a reasoned request, and taking into account whether the individual is represented by an attorney, interpretation at the arbitral hearing as well as translation of arbitral materials will be provided at no cost to the individual, unless the panel finds that, under the circumstances of the specific arbitration, this would lead to unjustified or disproportionate costs.
7. Materials submitted to arbitrators will be treated confidentially and will only be used in connection with the arbitration.
8. Individual-specific discovery may be permitted if necessary, and such discovery will be treated confidentially by the parties and will only be used in connection with the arbitration.
9. Arbitrations should be completed within 90 days of the delivery of the Notice to the organization at issue, unless otherwise agreed to by the parties.

H. Costs

Arbitrators should take reasonable steps to minimize the costs or fees of the arbitrations.

Subject to applicable law, the Department of Commerce will facilitate the establishment of a fund, into which Privacy Shield organizations will be required to pay an annual contribution, based in part on the size of the organization, which will cover the arbitral cost, including arbitrator fees, up to maximum amounts ("caps"), in consultation with the European Commission. The fund will be managed by a third party, which will report regularly on the operations of the fund. At the annual review, the Department of Commerce and European Commission will review the operation of the fund, including the need to adjust the amount of the contributions or of the caps, and will consider, among other things, the number of arbitrations and the costs and timing of the arbitrations, with the mutual understanding that there will be no excessive financial burden imposed on Privacy Shield organizations. Attorney's fees are not covered by this provision or any fund under this provision.

Concurring Statement

SEPARATE STATEMENT OF COMMISSIONER NOAH JOSHUA PHILLIPS

Despite representing that it would not share its users' health details with anyone, Flo Health, Inc. ("Flo") allegedly did so. As charged in the complaint, Flo coded app events, a mechanism by which app developers use third-party analytics to track how users use their apps, with words like "Pregnancy", and then shared them with analytics divisions of third parties including Facebook and Google.¹ I support this complaint and consent, which sends an important message about the care that app developers must take to level with users about how they share user data.

I write to respond to the vision my colleagues articulate about when the Commission should use consumer notice in our data security and privacy enforcement program.

The order that we place on the public record for comment requires Flo to seek deletion of data it improperly shared with third parties; obtain users' affirmative express consent before sharing their health information with third parties; report to the Commission future unauthorized disclosures; obtain an outside assessment of its privacy practices; and provide the following notice to consumers:

Between June 1, 2016 and February 23, 2019, the company that makes the Flo Period & Ovulation Tracker app sent an identifying number related to you and information about your period and pregnancy to companies that help us measure and analyze trends, usage, and activities on the app, including the analytics divisions of Facebook, Flurry, Fabric, and Google. No information was shared with the social media divisions of these companies. We did not share your name, address, or birthday with anyone at any time.²

In championing the consumer notice remedy in their concurring statement, Commissioners Chopra and Slaughter propose that the Commission no longer assess each case on its particular merits when determining when to order consumer notice.³ Rather, they assert that "the Commission should presumptively seek notice provisions in privacy and data security matters, especially in matters that do not include redress for victims."⁴ I disagree with that approach.

1 The Complaint does not challenge the use of third-party analytics services, upon which developers routinely rely. Because Flo Health coded events with names like "R_Pregnancy_Week_Chosen", rather than something generic like "Event 1", the events conveyed health information. The Wall Street Journal reported this conveyance on February 22, 2019, and the next day Flo Health ceased its conduct.

2 Consent, Exhibit A.

3 Commissioners Chopra and Slaughter also assert that the "plain language" of the Health Breach Notification Rule covers Flo. I disagree. We have never applied the Rule to a health app such as Flo in the past, in part because the language of the Rule is not so plain. And I do not support announcing such a novel interpretation of the Rule here, in the context of an enforcement action. See Joint Statement of Comm'r Chopra and Comm'r Slaughter, *In re Flo Health*, File No. 1923133 (Jan. 13, 2021).

4 *Id.*

Concurring Statement

The Commission has used notice requirements to prevent ongoing harm to consumers and to enable them to remediate the effects of harm suffered. To that end, the Commission has required consumer notice in cases where:

- consumers' health or safety is at risk;⁵
- consumers are subject to recurring charges that they may be unaware of;⁶
- consumers have a financial or legal interest that needs to be protected;⁷
- notice is necessary to prevent the ongoing dissemination of deceptive information;⁸ or
- consumers on their own would not have been able to discover or determine the illegal behavior and would not know to take remedial action.⁹

Using these guidelines, the Commission has found consumer notice appropriate in some privacy and data security cases as well, such as when there was a need to inform consumers about ongoing data collection and sharing¹⁰ or to correct a deceptive data breach notification.¹¹ On the data security front, where it can be critical that consumers know that sensitive information has been breached or exposed, a panoply of state breach notification laws require notice to consumers.

5 For example, in *Daniel Chapter One*, No. 9329 (Jan. 25, 2010) <https://www.ftc.gov/enforcement/cases-proceedings/082-3085/daniel-chapter-one>, the final order required the respondent to notify consumers that the company's cancer treatment claims regarding its dietary supplements were deceptive, and the supplements could actually interfere with cancer treatment.

6 For example, in the stipulated final order in *FTC v. Lumos Labs, Inc.*, No. 3:16-cv-0001, at 12-13, 22-23 (C.D. Cal. Jan. 8, 2016), the required notices described the FTC's allegations and explained how to cancel service.

7 In *FTC v. American Financial Benefits Center*, No. 4:18-cv-00806 (N.D. Cal. Feb. 7, 2018), consumers were notified that their recurring payments to the company were not being used to pay off their student loans.

8 In *FTC v. Applied Food Sciences, Inc.*, No. 1:14-cv-00851 at 12, 21 (W.D. Tex. Sept. 10, 2014), a wholesaler of dietary supplement ingredients distributed misleading information to supplement makers, touting the results of a clinical study that the FTC's investigation had shown to be botched. The company was required to notify all supplement makers who had received the misleading information that the FTC did not find the study credible.

9 For example, in *Oracle Corp.*, No. C-4571 (Mar. 29, 2016), <https://www.ftc.gov/enforcement/cases-proceedings/132-3115/oracle-corporation-matter>, the settlement required Oracle to notify consumers about certain data security risks and explain how to protect their personal information by deleting older versions of Java.

10 *Unrollme Inc.*, No. C-4692 (Dec. 17, 2019), <https://www.ftc.gov/enforcement/cases-proceedings/172-3139/unrollme-inc-matter>.

11 *Unrollme Inc.*, No. C-4692 (Dec. 17, 2019), <https://www.ftc.gov/enforcement/cases-proceedings/172-3139/unrollme-inc-matter>.

Concurring Statement

When warranted, notice to consumers can be an important tool. But neither the Commission, nor any of the 50 states with data breach notification laws, have taken the position of requiring consumer notice for the mere sake of the notice itself. Commissioners Chopra and Slaughter stress that notice is warranted especially where redress is not paid to consumers. How consumer notice substitutes for redress, an equitable mechanism to return to consumers what they have lost, is not clear. Nor is it clear what, if anything, limits this approach to notice to data security and privacy cases. To the extent notice is intended as a penalty, I disagree. My view is that we should target notice as a means to help consumers take action to protect themselves. Contacting consumers when there is no remedial action that they can take runs the risk of undermining consumer trust and needlessly overwhelming consumers.¹²

¹² I am also concerned about the possibility of notice fatigue. For example, in the context of security warnings on mobile devices, there is evidence of a decreased neurological response after repeated exposure to warnings. See, e.g., Anthony Vance et al., *Tuning Out Security Warnings: A Longitudinal Examination of Habituation Through fMRI, Eye Tracking, and Field Experiments*, 42 MIS Quarterly, No. 2, June 2018, at 1, https://misq.org/skin/frontend/default/misq/pdf/appendices/2018/V42I1Appendices/14124_RA_VanceJenkins.pdf.

Concurring and Dissenting Statement

JOINT STATEMENT OF COMMISSIONER ROHIT CHOPRA AND COMMISSIONER REBECCA KELLY SLAUGHTER CONCURRING IN PART, DISSENTING IN PART

Today, the FTC is ordering Flo Health, Inc. (“Flo”) to notify consumers that it has been charged with sharing consumers’ menstruation and fertility information without their consent. This proposed settlement is a change for the FTC, which has never before ordered notice of a privacy action. We commend the agency’s staff for securing this relief and for addressing Flo’s concerning practices.

While we are pleased to see this change, we are disappointed that the Commission is not using all of its tools to hold accountable those who abuse and misuse personal data. We believe that Flo’s conduct violated the Health Breach Notification Rule, yet the Commission’s proposed complaint fails to include this allegation. The rule helps ensure that consumers are informed when their data is misused, and firms like Flo should not be ignoring it.

Importance of Notice

Flo Health is the developer of a popular mobile app that collects menstruation and fertility information from millions of users worldwide. As detailed in the Commission’s complaint, Flo promised these users that it would not disclose their sensitive information to third parties, but did so anyway – sharing it with Facebook, Google, and others.¹ This alleged conduct broke user trust, and it broke the law.

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.²

1 Compl., In the Matter of Flo Health, Inc., Docket No. 1923133, ¶¶ 13-24.

2 In a separate statement, Commissioner Phillips argues that notice should be limited to circumstances under which it can “help consumers take action to protect themselves.” See Separate Statement of Commissioner Noah Joshua Phillips In the Matter of Flo Health, Inc. Comm’n File No. 1923133 at 2 (Jan. 13, 2021). In our view, the notice requirement here squarely meets that test, as consumers can switch to more privacy-protecting services or adjust their data-sharing behavior with companies that act unlawfully. Commissioner Phillips further suggests that notice is no substitute for redress. We agree. But when redress is not ordered, notice at least ensures consumers are aware of

the FTC’s action, which might otherwise be achieved through a redress check. Finally, Commissioner Phillips argues that consumers may not read all notices. This is a valid concern, and notice is no substitute for other remedies, such as admissions of liability or substantive limits on the collection, use, and abuse of personal data.

Concurring and Dissenting Statement

Health Breach Notification Rule

The Commission must also ensure it is vigorously enforcing the laws on the books. Congress has entrusted the FTC with promulgating and enforcing the Health Breach Notification Rule, one of only a handful of federal privacy laws protecting consumers. The rule requires vendors of unsecured health information, including mobile health apps, to notify users and the FTC if there has been an unauthorized disclosure. Although the FTC has advised mobile health apps to examine their obligations under the rule,³ including through the use of an interactive tool,⁴ the FTC has never brought an action to enforce it.⁵

In our view, the FTC should have charged Flo with violating the Health Breach Notification Rule. Under the rule, Flo was obligated to notify its users after it allegedly shared their health information with Facebook, Google, and others without their authorization.⁶ Flo did not do so, making the company liable under the rule.⁷

The Health Breach Notification Rule was first issued more than a decade ago, but the explosion in connected health apps make its requirements more important than ever. While we

3 *Mobile Health App Developers: FTC Best Practices*, FED. TRADE COMM’N, <https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-app-developers-ftc-best-practices> (last visited on Jul. 31, 2020).

4 *Mobile Health Apps Interactive Tool*, FED. TRADE COMM’N, <https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool> (last visited on Jul. 31, 2020).

5 Commissioner Phillips suggests that enforcing the rule against Flo would be “novel.” Phillips Statement, *supra* note 2, at 1. But, this could be said of any enforcement action in this context, since the Commission has never enforced the Health Breach Notification Rule. If there is concern that Flo did not know it was violating the rule, that would be relevant to the question of whether Flo is liable for civil penalties. See 15 U.S.C. § 45(m)(1)(A). Flo’s lack of knowledge about the rule’s requirements would not be relevant to the question of whether the Commission could charge Flo with a violation.

6 See Compl., *supra* note 1, ¶¶ 18-24. The FTC’s Health Breach Notification Rule covers (a) health care providers that (b) store unsecured, personally identifiable health information that (c) can be drawn from multiple sources, and the rule is triggered when such entities experience a “breach of security.” See 16 C.F.R. § 318. Under the definitions

cross-referenced by the Rule, Flo – which markets itself as a “health assistant” – is a “health care provider,” in that it “furnish[es] health care services and supplies.” See 16 C.F.R. § 318.2(e); 42 U.S.C. § 1320d(6), d(3). Additionally, Flo stores personally identifiable health information that is not secured according to an HHS-approved method, and that can be drawn from multiple source. See 16 C.F.R. § 318.2(i); *Fitness Trackers and Apps*, FLO HEALTH, <https://flo.health/faq/fitness-trackers-and-apps> (last visited on Jan. 6, 2020) (instructing users on how to sync Flo with other apps). When Flo, according to the complaint, disclosed sensitive health information without users’ authorization, this was a “breach of security” under the rule 16 C.F.R. § 318.2(a) (defining “breach of security” as “acquisition of [PHR identifiable health information] without the authorization of the individual.”)

7 See 16 C.F.R. § 318.7 (stating that a violation of the rule constitutes a violation of a trade regulation rule). Notably, California’s recent action against a similar fertility-tracking app charged with similar privacy violations included a \$250,000 civil penalty. Press Release, Cal. Att’y Gen., Attorney General Becerra Announces Landmark Settlement Against Glow, Inc. – Fertility App Risked Exposing Millions of Women’s Personal and Medical Information (Sep. 17, 2020), <https://oag.ca.gov/news/press-releases/attorney-general-becerra-announces-landmark-settlement-against-glow-inc-%E2%80%93>

Concurring and Dissenting Statement

would prefer to see substantive limits on firms' ability to collect and monetize our personal information, the rule at least ensures that services like Flo need to come clean when they experience privacy or security breaches. Over time, this may induce firms to take greater care in collecting and monetizing our most sensitive information.

Conclusion

We are pleased to see a notice provision in today's proposed order, but there is much more the FTC can do to protect consumers' data, and hold accountable those who abuse it. Where Congress has given us rulemaking authority, we should use it.⁸ And where we have rules already on the books, we should enforce them. Here, the Health Breach Notification Rule will have its intended effect only if the FTC is willing to enforce it.

We believe enforcing the rule was warranted here, and we respectfully dissent from the

Commission's failure to do so. Particularly as we seek more authority from Congress in the privacy space, it is critical we demonstrate we are prepared to use the authorities we already have.

⁸ We have previously articulated opportunities to make use of our existing authorities when it comes to data protection. See Statement of Commissioner Rohit Chopra Regarding the Report to Congress on the FTC's Use of Its Authorities to Protect Consumer Privacy and Security, Comm'n File P065404 (June 18, 2020), <https://www.ftc.gov/public-statements/2020/06/statement-commissioner-rohit-chopra-regarding-report-congress-ftcs-use-its>; Remarks of Commissioner Rebecca Kelly Slaughter at Silicon Flatirons, The Near Future of U.S. Privacy Law, University of Colorado Law School (Sep. 6, 2019), https://www.ftc.gov/system/files/documents/public_statements/1543396/slaughter_silicon_flatirons_remarks_9-6-19.pdf.

Analysis to Aid Public Comment

ANALYSIS OF CONSENT ORDER TO AID PUBLIC COMMENT

The Federal Trade Commission (the “Commission”) has accepted, subject to final approval, an agreement containing a consent order from Flo Health, Inc. (“Respondent” or “Flo Health”).

The proposed consent order (“Proposed Order”) has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission will again review the agreement, along with any comments received, and will decide whether it should withdraw from the agreement and take appropriate action or make final the Proposed Order.

This matter involves Flo Health, a technology start-up that develops and distributes a mobile application called the Flo Period & Ovulation Tracker (“App”), which collects and stores menstruation and fertility information about millions of users worldwide. 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.

The Commission’s proposed complaint alleges that Flo Health deceived consumers, in violation of Section 5(a) of the Federal Trade Commission Act, in seven ways:

- First, the complaint alleges that Flo Health represented that it would not disclose “information regarding ... marked cycles, pregnancy, symptoms, notes ...” to any third parties, or disclose “any data related to health” to particular third parties. In fact, Flo Health disclosed custom app events—records of individual users’ interactions with various features of the App, which conveyed identifying information about App users’ menstrual cycles, fertility, and pregnancies—to various third-party marketing and analytics firms.
- Second, the complaint alleges that Flo Health represented that it would *only* disclose device identifiers or personal data “like” device identifiers to certain third parties. In fact, in addition to disclosing device and advertising identifiers, Flo Health also disclosed custom app events conveying health information to those parties.
- Third, the complaint alleges that Flo Health represented that third parties would not use Flo App users’ personal information “for any purpose except to provide services in connection with the App.” In fact, Flo Health agreed to terms with multiple third parties that permitted these third parties to use Flo App users’ personal health information for the third parties’ own purposes, including for advertising and product improvement. Indeed, from June 2016 to February 2019, one of the third parties (Facebook, Inc.) used Flo App users’ personal health information for its own purposes, including its own research and product development.

Analysis to Aid Public Comment

- Counts IV through VII allege misrepresentations of compliance with the Privacy Shield Principles of Notice (Count IV), Choice (Count V), Accountability for Onward Transfers (Count VI), and Purpose Limitation (Count VII). Count IV alleges that Flo Health represented compliance with the Privacy Shield frameworks, when in fact it did not give Flo App users notice about to whom their data would be disclosed and for what purposes. Count V alleges that Flo Health disclosed this information without providing Flo App users with choice with respect to these disclosures or the purposes for which the data could be processed (e.g., Facebook’s advertising). Count VI alleges that Flo Health failed to limit by contract the third parties’ use of users’ health data or require by contract the third parties’ compliance with the Privacy Shield principles. And Count VII alleges that Flo Health processed users’ health data in a manner incompatible with the purposes for which it had been collected because Flo disclosed the data to third parties under contracts permitting them to use the data for their own purposes.

The Proposed Order contains injunctive provisions addressing the alleged deceptive conduct. Part I prohibits Flo Health from making false or deceptive statements regarding: (1) the purposes for which Flo Health or any entity to whom it discloses Covered Information (i.e., personal information, including identifiable health information) collects, maintains, uses, or discloses such information; (2) the extent to which consumers may exercise control over Flo Health’s access, collection, maintenance, use, disclosure, or deletion of Covered Information; (3) the extent to which Flo Health complies with any privacy, security, or compliance program, including the Privacy Shield; and (4) the extent to which Flo Health collects, maintains, uses, discloses, deletes, or permits or denies access to any Covered Information, or the extent to which Flo Health protects the availability, confidentiality, or integrity of Covered Information.

Part II of the Proposed Order requires Flo Health to ask any “Third Party” (i.e., any party other than Flo Health, its service providers, or subcontractors) that has received “Health Information” about “Covered App Users” to destroy such information.

Part III of the Proposed Order requires that Flo provide notice to users and the public that it shared certain information about users’ periods and pregnancies with the data analytics divisions (but not the social media divisions) of a number of third parties, including Facebook, Flurry, Fabric, and Google.

Part IV of the Proposed Order requires that, before disclosing any consumer’s health information to a third party, Flo Health must provide notice and obtain express affirmative consent, including informing the user of the categories of information to be disclosed, the identities of the third parties, and how the information will be used.

Part V of the Proposed Order requires an outside “Compliance Review,” conducted within 180 days after entry of the Proposed Order, to verify any attestations and assertions Flo Health made pursuant to the EU-U.S. Privacy Shield or the U.S.-Swiss Privacy Shield framework.

Analysis to Aid Public Comment

Part VI of the Proposed Order requires Flo Health to cooperate with the Compliance Reviewer and Part VII requires that a senior manager of Flo Health certify Flo Health's compliance with the Proposed Order.

Part VIII of the Proposed Order requires notification of the Commission following any "Covered Incident," which includes any incident in which Flo Health disclosed individually identifiable Health Information from or about a consumer to a third party without first receiving the consumer's affirmative express consent.

Parts IX through XII of the Proposed Order are reporting and compliance provisions, which include recordkeeping requirements and provisions requiring Flo Health to provide information or documents necessary for the Commission to monitor compliance with the Proposed Order. Part XIII states that the Proposed Order will remain in effect for twenty (20) years, with certain exceptions.

The purpose of this analysis is to aid public comment on the Proposed Order. It is not intended to constitute an official interpretation of the complaint or Proposed Order, or to modify in any way the Proposed Order's terms.

Complaint

IN THE MATTER OF

KUSHLY INDUSTRIES LLC**AND****CODY ALT**CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF SECTIONS 5 AND 12 OF THE
FEDERAL TRADE COMMISSION ACT*Docket No. C-4749; File No. 202 3111**Complaint, June 29, 2021– Decision, June 29, 2021*

This consent order addresses Kushly Industries LLC’s advertising of products containing cannabidiol. The complaint alleges that Respondents violated Sections 5(a) and 12 of the Federal Trade Commission Act by disseminating false and unsubstantiated advertisements that claimed that: (1) CBD Products effectively treat, mitigate, or cure diseases or health conditions including: sleep disorders, including insomnia and narcolepsy; psychiatric disorders, including depression, bipolar disorder, post-traumatic stress disorder, psychosis, and anorexia nervosa; cancer; multiple sclerosis; Parkinson’s disease; hypertension; Alzheimer’s disease; acne, psoriasis, eczema; arthritis; muscle spasms; pain resulting from endometriosis; and dysmenorrhea; and (2) studies or scientific research prove that CBD Products effectively treat, mitigate, or cure multiple sclerosis, general anxiety disorder, post-traumatic stress disorder, panic disorder, obsessive-compulsive disorder and social anxiety disorder, depression, cancer, sleep disorders, hypertension, Parkinson’s disease, Alzheimer’s disease, acne, psoriasis, and eczema, and improve sleep. The consent order prohibits Respondents from making any representation about the efficacy of any covered product, including that such product effectively treats, mitigates, or cures diseases or health conditions including: sleep disorders, including insomnia and narcolepsy; headaches; psychiatric disorders, including depression, bipolar disorder, general anxiety disorder, panic disorder, obsessive-compulsive disorder and social anxiety disorder; post-traumatic stress disorder, psychosis, and anorexia nervosa; cancer; multiple sclerosis; chronic drowsiness; Parkinson’s disease; hypertension; Alzheimer’s disease; acne, psoriasis, eczema; arthritis; muscle spasms; pain resulting from endometriosis; and dysmenorrhea, unless the representation is non-misleading, including that, at the time such representation is made, they possess and rely upon competent and reliable scientific evidence that substantiates that the representation is true.

Participants

For the *Commission*: Luis Gallegos and Reid Tepfer.

For the *Respondents*: David Rossiter Callaway, Goodwin Procter LLP.

COMPLAINT

The Federal Trade Commission, having reason to believe that Kushly Industries LLC, a limited liability company, and Cody Alt, individually and as an officer of Kushly Industries LLC (collectively, “Respondents”), have 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 Kushly Industries LLC (“Kushly”) is an Arizona limited liability company with its principal office or place of business at East Rancho Vista Drive, #3014, Scottsdale, Arizona 85251.