6750-01-P]

FEDERAL TRADE COMMISSION

[File No. 192 3133]

Flo Health, Inc.; Analysis of Proposed Consent Order to Aid Public Comment

AGENCY: Federal Trade Commission.

ACTION: Proposed consent agreement; request for comment.

SUMMARY: The consent agreement in this matter settles alleged violations of federal law prohibiting unfair or deceptive acts or practices. The attached Analysis of Proposed Consent Order to Aid Public Comment describes both the allegations in the draft complaint and the terms of the consent order—embodied in the consent agreement—that would settle these allegations.

DATES: Comments must be received on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]**.

ADDRESSES: Interested parties may file comments online or on paper by following the instructions in the Request for Comment part of the **SUPPLEMENTARY INFORMATION** section below. Please write "Flo Health, Inc.; File No. 192 3133" on your comment, and file your comment online at *https://www.regulations.gov* by following the instructions on the web-based form. If you prefer to file your comment on paper, mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Suite CC-5610 (Annex D), Washington, DC 20580, or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Constitution Center, 400 7th Street SW, 5th Floor, Suite 5610 (Annex D), Washington, DC 20024.

FOR FURTHER INFORMATION CONTACT: Elisa Jillson (202-326-3001), Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

SUPPLEMENTARY INFORMATION: Pursuant to Section 6(f) of the Federal Trade Commission Act, 15 U.S.C. 46(f), and FTC Rule 2.34, 16 CFR 2.34, notice is hereby given that the above-captioned consent agreement containing a consent order to cease and desist, having been filed with and accepted, subject to final approval, by the Commission, has been placed on the public record for a period of thirty (30) days. The following Analysis to Aid Public Comment describes the terms of the consent agreement and the allegations in the complaint. An electronic copy of the full text of the consent agreement package can be obtained at *https://www.ftc.gov/news-events/commission-actions*.

You can file a comment online or on paper. For the Commission to consider your comment, we must receive it on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]**. Write "Flo Health, Inc.; File No. 192 3133" on your comment. Your comment—including your name and your state—will be placed on the public record of this proceeding, including, to the extent practicable, on the *https://www.regulations.gov* website.

Due to the COVID-19 pandemic and the agency's heightened security screening, postal mail addressed to the Commission will be subject to delay. We strongly encourage you to submit your comments online through the *https://www.regulations.gov* website.

If you prefer to file your comment on paper, write "Flo Health, Inc.; File No. 192 3133" on your comment and on the envelope, and mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Suite CC-5610 (Annex D), Washington, DC 20580; or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Constitution Center, 400 7th Street SW, 5th Floor, Suite 5610 (Annex D), Washington, DC 20024. If possible, submit your paper comment to the Commission by courier or overnight service.

Because your comment will be placed on the publicly accessible website at *https://www.regulations.gov*, you are solely responsible for making sure your comment does not include any sensitive or confidential information. In particular, your comment should not include sensitive personal information, such as your or anyone else's Social Security number; date of birth; driver's license number or other state identification number, or foreign country equivalent; passport number; financial account number; or credit or debit card number. You are also solely responsible for making sure your comment does not include sensitive health information, such as medical records or other individually identifiable health information. In addition, your comment should not include any "trade secret or any commercial or financial information which . . . is privileged or confidential"—as provided by Section 6(f) of the FTC Act, 15 U.S.C. 46(f), and FTC Rule 4.10(a)(2), 16 CFR 4.10(a)(2)—including in particular competitively sensitive information such as costs, sales statistics, inventories, formulas, patterns, devices, manufacturing processes, or customer names.

Comments containing material for which confidential treatment is requested must be filed in paper form, must be clearly labeled "Confidential," and must comply with FTC Rule 4.9(c). In particular, the written request for confidential treatment that accompanies the comment must include the factual and legal basis for the request, and must identify the specific portions of the comment to be withheld from the public record. *See* FTC Rule 4.9(c). Your comment will be kept confidential only if the General Counsel grants your request in accordance with the law and the public interest. Once your comment has been posted on the *https://www.regulations.gov* website—as legally required by FTC Rule 4.9(b)—we cannot redact or remove your comment from that website, unless you submit a confidentiality request that meets the requirements for such treatment under FTC Rule 4.9(c), and the General Counsel grants that request.

Visit the FTC Website at *http://www.ftc.gov* to read this Notice and the news release describing the proposed settlement. The FTC Act and other laws that the Commission administers permit the collection of public comments to consider and use in this proceeding, as appropriate. The Commission will consider all timely and responsive public comments that it receives on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]**. For information on the Commission's privacy policy, including routine uses permitted by the Privacy Act, see *https://www.ftc.gov/site-information/privacy-policy*.

Analysis of Proposed 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 from 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.
- 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. 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.

By direction of the Commission, Commissioners Chopra and Slaughter concurring in part and dissenting in part.

Joel Christie,

Acting Secretary.

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 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 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

[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.

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 "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.

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

---

[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*.

[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.

- 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 sharing[10] or to correct a deceptive data breach notification.[11] On the data security front, where it can be critical that consumers know sensitive information has been breached or exposed, a panoply of state breach notification laws require notice to consumers.

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]

---

[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] *Skymed International, Inc.,* File No. 1923140 (Dec. 16, 2020), https://www.ftc.gov/enforcement/cases-proceedings/1923140/skymed-international-inc-matter.

[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.

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

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

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]

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

---

[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.

[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, s*upra* 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.

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 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.

---

[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 CFR 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 CFR 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 CFR § 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 CFR 318.2(a) (defining "breach of security" as "acquisition of [PHR identifiable health information] without the authorization of the individual.")

[7] *See* 16 CFR 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.

[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.

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.

[FR Doc. 2021-01697 Filed: 1/27/2021 8:45 am; Publication Date: 1/28/2021]