WORLD **PRIVACY** FORUM

Comments of the World Privacy Forum to the Federal Trade Commission regarding
Proposed Consent Order, *In the Matter of Flo Health, Inc., File No. 1923133*

Via regulations.gov

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW
Suite CC-5610 (Annex D)
Washington DC, 20580

1 March, 2021

Dear Commissioners:

Thank you for the opportunity to comment on the proposed consent order in the matter of Flo Health, Inc., File No. 1923133. (https://www.ftc.gov/enforcement/cases-proceedings/1923133/flo-health-inc)The World Privacy Forum is a non-profit public interest research group focused on privacy issues, including health privacy. We have published extensively in the health privacy area, including *A Patient's Guide to HIPAA*, (https://www.worldprivacyforum.org/2019/03/hipaa/) extensive material about medical identity theft, (https://www.worldprivacyforum.org/category/med-id-theft/) extensive material about electronic health records, (https://www.worldprivacyforum.org/category/electronic-health-records/) among other health privacy and data governance topics. WPF is a member of the World Health Organization's HDC, and serves on its data governance committee. For more information, see www.worldprivacyforum.org.

We agree with the FTC's analysis regarding Flo Health, Inc.'s violations of parts of the EU-US Privacy Shield framework, the US-Swiss Privacy Shield framework, and Section 5a of the FTC Act.

However, we have questions about the FTC's decision to not require notification in regards to the FTC Health Breach Notification Rule, which implements section 13407

of the American Recovery and Reinvestment Act of 2009. The FTC's version of the Health Data Breach Rule does not apply to covered entities under HIPAA, nor does it apply to Business Associates under the HIPAA Rule. Instead, the FTC Health Breach Notification Rule is narrowly crafted. According to the confines of the Rule's definitions, in order for its activity to be covered under the Rule, Flo Health would have had to provide services to a vendor of PHRs or to a PHR-related entity in connection with a product or service offered by that entity. It is possible that the question of whether or not Flo Health qualifies under the FTC Health Data Breach Notification Rule depends on the narrow issue of whether or not Flo Health allowed its data to be added directly to a PHR or to be utilized in connection with a PHR-related entity.

Our analysis is that Flo's activities may very narrowly qualify as falling under the FTC's Health Data Breach Notification Rule.

If one or more Flo Health users imported Flo Health data to their own PHR(s) or to digital health record(s) they held, for example, on a mobile device or a fitness tracking device, then Flo Health could potentially fall under the FTC Health Data Breach Notification rule. The narrow intersection of coverage of the Rule may occur where Flo Health data can be synced with Fitbit. This relationship is consequential, because Flo could reasonably be characterized as providing services to a PHR-related entity in connection with a product or service offered by that entity as a result.[1]

In its settings menu within the app, Flo Health has specific settings where users can connect Flo to Fitbit. Flo has help pages advising users about how the steps they need to take to register their Fitbit account in the Flo Menu Profile. (https://help.flo.health/hc/en-us/articles/360015330671-My-Fitbit-won-t-sync). Similarly, Fitbit for its part lists Flo Health as one of its "Works with Fitbit" providers. (https://www.fitbit.com/global/us/technology/partnership).

Fitbit could be characterized as a PHR-related entity for multiple reasons. One reason is the acquisition of Twine by Fitbit in 2018. Twine data comes from a variety of connected medical devices, and from electronic health (medical) records that users report (which in most cases makes the record a personal health record, or PHR.) Additionally, Fitbit is associated with many workplace health programs, which also can in some instances call in interactions with a PHR.

Fifteen years ago, providing services to a PHR-related entity in connection with a service offered by that entity was a much more difficult task. The technology was often clunky, and data transfers could be challenging. Today, though, there is much greater

---

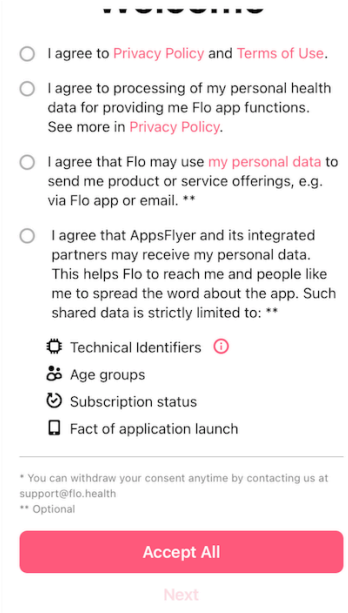
[1] The FTC Health Data Breach Notification Rule defines a PHR as: Personal health record means an electronic record of PHR identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual. §318.2 (d). https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=1&SID=6ae79a215bd299fd401a63594e98ce70&ty=HTML&h=L&n=16y1.0.1.3.42&r=PART#se16.1.318_12.

maturity and sophistication in the integration of smartwatches, mobile trackers, and personal health records.

The significant loss of friction of these types of data transfers has caused the definitions that were crafted so narrowly when the FTC wrote its original rule to escape their boundaries by virtue of these developments. While the applicability of the Rule is very narrow, in our analysis, it nonetheless appears to apply. We urge the FTC to take another look at this particular aspect of the proposed agreement.

Additional concerns

In researching the Flo app, our experience with the app was that even though some sharing, such as the AppsFlyer sharing, was stated as optional, it did not appear to be possible to avoid consenting at the time of notification. In order to opt out of the consent, users are told that "*You can withdraw your consent anytime by contacting us at support@flo.health." (The screenshot below was taken 1 March, 2020.)



The FTC has recommended a variety of mobile notice best practices in its report, *Mobile Privacy Disclosures*. (https://www.ftc.gov/news-events/press-releases/2013/02/ftc-staff-report-recommends-ways-improve-mobile-privacy). In this report, the FTC recommended "just in time" disclosures and obtaining affirmative express consent before allowing apps to access sensitive content. We support the idea of just in time disclosures and consent for mobile privacy notifications, and in line with the FTC's report, we think it would be a good practice to allow consumers to be notified about the AppsFlyer sharing ***and*** have the ability to decline consent for that sharing on the very same screen at that time, instead of directing consumers to write an email to support personnel after the fact to request an opt out.

Conclusion

In conclusion, we urge the FTC to take another look at whether or not the FTC's Health Data Breach Notification Rule would apply in this instance, understanding that that analysis is narrow.

We also request that the compliance reports the FTC is requiring from Flo Health be made public proactively, so that it does not require a FOIA process to see the reports. This is important because Flo Health claims to have in excess of a hundred million downloads of its app. If so, then these privacy reports from Flo Health are of high interest to the public, and should be made public as part of the consent agreement.

Thank you for your work.

Respectfully submitted,

Pam Dixon
Executive Director,
World Privacy Forum