UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Office of Commissioner
Rohit Chopra

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

In the Matter of Flo Health, Inc.
Commission File No. 1923133

January 13, 2021

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

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]

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.

[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.

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.

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.