BRIAN M. BOYNTON
Principal Deputy Assistant Attorney General
Civil Division
ARUN G. RAO
Deputy Assistant Attorney General
AMANDA N. LISKAMM
Director
LISA K. HSIAO
Assistant Director
RACHEL E. BARON
Trial Attorney
Consumer Protection Branch
U.S. Department of Justice
Civil Division

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS

UNITED STATES OF AMERICA, Plaintiff, v. EASY HEALTHCARE CORPORATION., a corporation, d/b/a EASY HEALTHCARE, Defendant	**Case No. 1:23-cv-3107** **COMPLAINT FOR PERMANENT INJUNCTION, CIVIL PENALTY JUDGMENT, AND OTHER RELIEF**

Plaintiff, the United States of America, acting upon notification and authorization to the Attorney General by the Federal Trade Commission ("FTC"), pursuant to Section 16(a)(1) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 56(a)(1), for its Complaint alleges:

1. Plaintiff brings this action under Sections 5(a)(1), 5(m)(1)(A), 13(b), 16(a)(1), and 19 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §§ 45(a)(1), 45(m)(1)(A), 53(b), 56(a)(1), 57b, which authorize the Plaintiff to seek, and the Court to order, permanent injunctive relief, civil penalties, and other relief for Defendant's acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), and in violation of the Health Breach Notification Rule (the "Rule" or the "HBNR"), 16 C.F.R. § 318.

SUMMARY OF THE CASE

2. Defendant Easy Healthcare Corporation ("Defendant" or "Easy Healthcare") has developed, advertised, and distributed a mobile application ("app") called the Premom Ovulation Tracker ("Premom") that allows users to input and track various types of personal and health information. For example, users can log information about their periods and fertility and upload pictures of ovulation test strips that the app can analyze to attempt to predict the user's next ovulation cycle. Defendant also designed Premom to permit users to import their health data from other devices or apps.

3. Hundreds of thousands of women have downloaded and used Premom, giving Defendant access to their mobile phones and their health information and other personal data. Between 2017 and 2020, Defendant repeatedly and falsely promised Premom users in their privacy policies that Defendant: (a) would not share health information with third parties without users' knowledge or consent; (b) to the extent Defendant collected and shared any information, it was non-identifiable data; and (c) the data was used only for Defendant's own analytics or advertising. Further, its privacy policies over time promised that Defendant would otherwise notify and obtain consent from users before using its users' data for any other purposes.

4. These representations were false or deceptive. Since 2018, Defendant has shared Premom users' identifiable health information with Google, LLC ("Google") and marketing firm AppsFlyer Inc. ("AppsFlyer"). This sharing was contrary to Defendant's promises to users and thus constitutes a breach of unsecured health information that requires notice to Premom users under the Health Breach Notification Rule. Because Defendant has not provided timely and proper notice to consumers, the FTC, or the media of this sharing, Defendant is in violation of the FTC Act and the Health Breach Notification Rule.

5. In addition to sharing users' sensitive health information with Google and AppsFlyer, between 2018 and 2020, Defendant shared users' sensitive, identifiable data with foreign mobile analytics companies Jiguang (also known as Aurora Mobile Ltd.) and Umeng. Defendant took no action to limit what these companies could do with their users' information. Rather, it merely agreed to each company's standard terms of service, all of which gave these companies broad latitude to use the data as they saw fit, including for advertising.

6. Defendant continued to share users' sensitive, identifiable data with Jiguang and Umeng, while promising privacy to its users, until the summer of 2020. At that time, the Google Play Store informed Defendant that its transfer of data to Umeng violated the Play Store policies, and separately the *Washington Post* reached out to Defendant for comment related to an article detailing their data practices.

7. In addition to making these false and deceptive representations to consumers, Defendant failed to implement reasonable privacy and data security measures. Because of these failures, Defendant shared Premom users' data with third parties in violation of Section 5 of the

FTC Act and, and failed to provide notice to consumers, the FTC, and the media of a breach of unsecured health information in violation of the Health Breach Notification Rule.

JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1337(a), and 1345.

9. Venue is proper in this District under 28 U.S.C. §§ 1391(b)(1), (b)(2), (c)(1), (c)(2), and (d), and 15 U.S.C. § 53(b).

DEFENDANT

10. Defendant Easy Healthcare Corporation ("Easy Healthcare") is an Illinois corporation with its principal office or place of business at 360 Shore Dr. Unit B, Burr Ridge, IL 60527. Easy Healthcare transacts or has transacted business in this District and throughout the United States. Easy Healthcare has developed and published Premom, an app that functions as an ovulation tracker, period tracker, and pregnancy resource for those who are trying to conceive.

COMMERCE

11. At all times relevant to this Complaint, Defendant has maintained a substantial course of trade in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

THE PREMOM APP

12. At all times relevant to this Complaint, Defendant has developed, advertised, and distributed Premom, which functions as an ovulation tracker, period tracker, and pregnancy resource for those who are trying to conceive.

13. Since at least 2017, Defendant has made Premom available to users for free download from the Apple App Store and the Google Play Store. In the product description on the Google Play Store, Defendant has described Premom as "the most accurate and reliable period tracker, ovulation calculator, and fertility calendar" and "the only fertility tracker and ovulation app that offers a pregnancy guarantee to help women who are trying to conceive (TTC) make their baby dreams come true." Hundreds of thousands of users have downloaded and used Premom.

14. Premom is designed to be used with ovulation test strips, which Easy Healthcare also produces and sells. Defendant's ovulation test kits have consistently ranked as a number one best seller on Amazon.com, and the test kits encourage purchasers to download the Premom app.

15. Defendant encourages women trying to conceive to upload pictures of ovulation tests and input large amounts of health information into the app. Premom's description in the Apple App Store states: "Track your symptoms and activities - period, moods, sex, sleep, cervix mucus, and more." Defendant further states in its Google Play Store description that "Our automatic ovulation test reader with ovulation test kits (OPK), offers optimized fertility predictions you can trust." For instance, while using the app, Premom asks users to input the dates they started their periods and upload results of progesterone tests.

16. In Premom's description in the Google Play Store and Apple App Store, Defendant further encourages women to connect Premom to third-party apps and products so that Premom can import health information from those apps or products. Specifically, Premom users can import their body temperatures, along with the date and time that the temperature is

taken, from the Apple Health app. Users can also import their body temperatures from thermometers that connect to Premom via Bluetooth.

17. Through Premom, Defendant has collected extensive sensitive personal health information about consumers, including dates of menstrual cycles, temperatures, pregnancy and fertility status, whether and when pregnancies started and ended, weight, progesterone and other hormone results, and pregnancy-related symptoms. Defendant also tells users that users can infer other facts about their health from this information, such as whether they suffer from conditions like Polycystic Ovary Syndrome or hormonal imbalances.

DEFENDANT MADE DECEPTIVE REPRESENTATIONS AND OMISSIONS ABOUT ITS INFORMATION COLLECTION, SHARING, AND USE PRACTICES

18. Since 2017, Defendant repeatedly falsely promised Premom users in their in-app and website privacy policies that Defendant (a) would not share health information with third parties; (b) to the extent Defendant collected and shared any information, it was non-identifiable data; and (c) the data was used only for Defendant's own analytics or advertising.

19. First, between April 2019 and September 2020, Defendant repeatedly stated in multiple in-app privacy policies that it would not share any health information with third parties without user consent. For example, in a privacy policy dated July 7, 2020, Defendant stated in a paragraph set off from other paragraphs: "WE PROMISE WE WILL NEVER SHARE YOUR EXACT AGE OR ANY DATA RELATED TO YOUR HEALTH WITH ANY THIRD PARTIES WITHOUT YOUR CONSENT OR KNOWLEDGE."

20. Second, since at least December 13, 2021, Defendant has stated in their in-app and website privacy policy that "Premom uses AppsFlyer, a mobile marketing platform based in the United States, to handle non-health Personal Data" and that "third party services do not have

access to your health information through the Services unless you share that information directly with them."

21. Third, Defendant also represented that it would share only "non-identifiable data" with third parties. Between May 2017 and July 2020, Premom's privacy policy posted on its website represented that it collected and shared Premom users' "nonidentifiable information for purposes of tracking analytics of the usage of [its] application." Premom's privacy policy represented that its use of third-party analytics software and software development kits "identifies a user solely by IP address."

22. Fourth, when a user wanted to connect a Bluetooth thermometer to Premom, Defendant prompted users with the following statement: "Please allow Premom to access your location and turn on the GPS for Bluetooth so it can find your thermometer" and asked users to "Allow Premom to access this device's location?" However, Defendant did not disclose in this prompt that it shared Premom users' location information with third parties.

23. Finally, Defendant represented that Premom users' data would be used only for Defendant's own analytics and advertising. Between May 2017 and July 2020, the privacy policy posted on Premom's website stated that it collected users' data to "[c]ustomize, measure and improve our services, content and advertising," and to "[e]valuate your use, preferences and trends for our own internal statistical and analytical purposes which we may use for marketing purposes. . . ." Defendant further represented that it "will not use your personal information for any purposes, other than those outlined in" Defendant's privacy policy or terms of service.

24. As described below, each of these representations or omissions made by Defendant was false or misleading.

DEFENDANT SHARED PREMOM USERS' HEALTH INFORMATION THROUGH CUSTOM APP EVENTS

25. Defendant integrated into the Premom app software development tools, known as software development kits ("SDKs"), from numerous third-party marketing and analytics firms. These SDKs provide functions for Defendant, such as enabling Defendant to track and analyze Premom users' interactions with Premom. By integrating these SDKs into Premom, Defendant would transfer its app users' data to the publisher of each SDK.

26. In fact, Defendant has incorporated SDKs from Google and AppsFlyer into the Premom app and disclosed health information to them through "Custom App Events."

27. Defendant tracks "Standard App Events," which are records of routine app functions, such as launching or closing the app, as well as "Custom App Events," which are records of user-app interactions unique to Premom. For example, when a user uploads a picture of an ovulation test, Defendant records the user's interaction with that feature as a Custom App Event that is shared with Google and AppsFlyer.

28. Rather than giving its Custom App Events anonymous names, Defendant chooses descriptive titles that convey health information about Premom users. For example, when a user opens Premom's calendar and logs her fertility, Defendant records the Custom App Event as "Calendar/Report/LogFertility." When a user signs up for Defendant's pregnancy guarantee, which promises to refund a Premom user's purchases of their ovulation and pregnancy test kits if a user does not successfully conceive within nine months of using Premom, Defendant records the Custom App Event as "Guarantee/signup." And when a user logs and saves information related to her period, Defendant records the Custom App Event as "Log period-save." Defendant chose other descriptive titles such as "Signup/Birth" and "Ovulation/Static/Success."

By sharing these Custom App Events with either AppsFlyer or Google, Defendant consequently conveyed information about users' fertility and pregnancies.

29. By including sensitive health information in the titles of the Custom App Events it has shared through third-party SDKs, Defendant has conveyed the health information of hundreds of thousands of users to these third parties for years. Through these SDKs, Defendant has also collected and shared Premom users' unique advertising or device identifiers. As described below in Paragraphs 36 through 38, third parties can use device identifiers to track consumers across the internet and apps, and eventually—through their own lists or by using a third-party service—match these identifiers to an actual person. Ultimately, this could allow these third parties to associate these fertility and pregnancy Custom App Events to a specific individual.

30. Defendant's transfers of these Custom App Events directly contradict Defendant's statements in their privacy policies that it would not share health information with third parties without users' knowledge or consent.

31. Defendant has never provided notice to Premom users of these unauthorized disclosures.

DEFENDANT SHARED CONSUMERS IDENTIFIABLE INFORMATION WITH THIRD PARTIES

32. Despite their assertions between 2018 and 2020 that their analytics software "identifies a user solely by IP address" and that it shared only *non-identifiable data* with third parties, Defendant—through the use of SDKs—collected and shared more than IP addresses, including information that could be used to identify Premom's users and disclose to third parties that these users were utilizing a fertility app.

33. Over various time periods since 2018, Defendant has incorporated into Premom the SDKs of, *inter alia*, Umeng, a Chinese mobile app analytics provider owned by the Chinese technology conglomerate Alibaba, and Jiguang, a Chinese mobile developer and analytics provider. Specifically, Defendant integrated U-Share and JPush, the SDKs marketed by Umeng and Jiguang respectively, into Premom.

34. Through the U-Share SDK, Defendant shared social media account information of Premom users with Umeng. By incorporating U-Share into Premom and sharing Premom users' social account information to Umeng, Defendant shared sensitive data that identifies its users.

35. Furthermore, the U-Share and JPush SDKs collected extensive amounts of other identifiable data on Premom's users and transmitted it to Umeng and Jiguang, including:

a) resettable identifiers such as Android ID and Android Advertising ID—which are a combination of numbers and letters assigned by a mobile phone to a user that can be used for targeted advertising—and phone Wi-Fi Media Access Control (MAC) addresses, which are identifiers for devices on a network;

b) non-resettable identifiers, such as:

i) Hardware Identification (HWID) and International Mobile Equipment Identity (IMEI) numbers—which are a set of numbers and letters that are unique and identify a computer or mobile phone;

ii) router, Bluetooth, and Wi-Fi Media Access Control (MAC) addresses—which are unique numbers hardcoded to those

devices—of devices on the network to which Premom users connected; and

iii) router Service Set Identifiers (SSIDs)—which are the names of your wireless network—and Bluetooth names—which contain identifying information, such as "Baker Family Wifi" or "Robert's Phone;" and

c) precise geolocation information—including Global Positioning System (GPS) coordinates information.

36. Companies can track consumers across the internet and devices via these resettable and non-resettable identifiers. A company can use these identifiers to track a consumer across apps and devices, and to collect other information about them that, in combination with these identifiers, can be used to identify particular individuals. Notably, non-resettable device identifiers, such as a device's IMEI are hardcoded to the device or network and, as a result, consumers concerned about tracking cannot disassociate themselves from their previous tracking history. Once a non-resettable identifier is linked to a consumer, that consumer cannot disassociate from the identifier without incurring great costs, such as needing to acquire a new phone or Wi-Fi router. In contrast, resettable identifiers permit consumers concerned about tracking to disassociate themselves from their previous tracking history by resetting the advertising identifier in either Apple's iOS or Google's Android settings. In doing so, the consumer would receive a new advertising identifier.

37. For example, through an SDK, a third party may receive information that a consumer with an advertising ID X12345 and an IMEI ABC6789 used the Premom app. Later,

that same third party may receive information that a consumer with an IMEI ABC6789 also used an app for weight loss. And sometime later, that same third party may receive information that a consumer with an advertising ID X12345 is using a smoking cessation app. The third party now knows that the same consumer (with an advertising ID X12345 and IMEI ABC6789) used a fertility app, a weight loss app, and a smoking cessation app. And while a consumer can disassociate themselves from advertising ID X12345, they cannot disassociate themselves from IMEI ABC6789 without purchasing a new mobile device.

38. Through the use of matching lists or through third-party services, a third-party can link these identifiers to a real person. Many surveillance advertising businesses specialize in tracking consumers' devices, collecting information on consumers, and identifying the consumer behind the device using this data, as well as connecting that consumer to other devices. Non-resettable identifiers are particularly important to the surveillance advertising industry. So, if a consumer provides their name in connection with an app that collects such resettable and non-resettable identifiers, or logs in to a major platform that shares such identifying information, then a third-party surveillance company or data broker can connect such identifiers to a person's name or identifying information. As such, a third party may learn that a user associated with advertising ID X12345 and IMEI ABC6789 is actually Jane Doe, and thereafter, the third party will know that Jane Doe uses Premom, a weight loss app, and a smoking cessation app.

39. In addition, when device identifiers are associated with precise geolocation data, the data becomes even more identifiable. With only a few location signals and a device identifier, third parties can identify a consumer's home address and identify other sensitive information about consumers, such as a consumer's healthcare provider or place of work. As

such, through data shared through an SDK, a third party may learn that the user associated with advertising ID X12345 and IMEI ABC6789 spends every evening at 123 Main St., and thereafter, the third party will know that Jane Doe uses Premom, a weight loss app, and a smoking cessation app, and lives at 123 Main St.

40. In addition to violating their promises to consumers, Defendant's contracts with Umeng and Jiguang and sharing of this information with Umeng and Jiguang violated Apple and Google policies. Jiguang disclosed in its privacy policy that Jiguang collected Wi-Fi MAC addresses and Defendant reviewed and agreed to Jiguang's privacy policy before incorporating the JPush SDK. Both Apple and Google contractually prohibit application developers from correlating, or syncing, the device advertising identifier with other identifiers, and from allowing third parties to obtain the advertising identifier via the application. Apple specifically forbids the collection of non-resettable device identifiers. Similarly, Google's Developer Policies state that in order to "protect user privacy," the Android Advertising ID "must not be connected to personally-identifiable information or associated with any persistent device identifier . . . without explicit consent of the user" and it restricts "access to MAC addresses." Typically, only a privileged app (e.g., a pre-installed app) can have access to the Wi-fi MAC address. However, the JPush SDK circumvented Android's privacy controls and exploited a known bug in order to acquire Premom users' Wi-fi MAC addresses.

41. Defendant did not just share sensitive, identifiable data with Umeng and Jiguang; it also knew that Umeng and Jiguang could use this data for their own business purposes or could transfer the data to additional third parties, and failed to disclose this information to Premom users. In fact, prior to incorporating each of these SDKs, Defendant reviewed and agreed to

Umeng's and Jiguang's terms of service and privacy policies. Each terms of service and privacy policy allowed these third parties to use and share Premom users' information for any of their own business purposes, including advertising. Since at least 2019, Umeng's privacy policies have stated that Umeng has the right to use data collected through U-Share for advertising purposes and transfer the data to its advertising and media partners. Likewise, since at least 2019, Jiguang's privacy policies have also stated that Jiguang may share the data collected through the "JPush" SDK with third parties.

42. Defendant never disclosed to Premom users that Jiguang could share data collected through the JPush SDK with third parties. Additionally, until July 2020, Defendant did not disclose that Umeng could share Premom user data with its partners. Defendant only made such a disclosure regarding Umeng after Google notified Defendant that their use of U-Share violated Google Play Store policies.

43. Altogether, the collection and sharing of the mobile device identifiers, and in particular the non-resettable identifiers described in Paragraphs 31 to 38, 40, and 41, enables third parties to circumvent operating system privacy controls, track individuals, infer the identity of an individual user, and ultimately associate the use of a fertility app to that user. The collection of social media account information described in Paragraph 34 also enables third parties to identify individual users and associate the use of a fertility app to that user. This directly contradicted Defendant's statements in their privacy policies that it would identify "a user solely by IP address" and share only "non-identifiable data" with third parties.

44. When Defendant sought Premom users' permission to access their location in order to pair a Bluetooth thermometer, as described in paragraph 22, it failed to disclose that it

collected and shared precise geolocation information with Umeng and Jiguang, as described in Paragraph 35. Nor did Defendant disclose that Umeng and Jiguang could use and transfer this information for their own purposes, such as third-party advertising.

45. In addition, by providing data to third parties that explicitly reserved the right to use such data for third party advertising, Defendant directly contradicted its own statements that it would use Premom users' data only for their own analytics and advertising.

DEFENDANT FAILED TO IMPLEMENT REASONABLE PRIVACY AND DATA SECURITY MEASURES

46. Defendant failed to take reasonable measures to assess and address privacy risks to user information while creating and maintaining Premom. For example:

a) Defendant failed to adequately assess the privacy risks of third-party SDKs prior to incorporating those SDKs into Premom;

b) Defendant failed to monitor changes in the privacy policies and terms and conditions of the SDK publishers as those publishers changed their data collection practices and updated their policies and terms; failed to engage in any audits, assessments, compliance reviews, or tests—including any tests to determine what data was transferred to third parties—regarding the data collection and privacy practices of the third-party publishers whose SDKs it incorporated into Premom; and failed to update their privacy practices to reflect changes that affected Premom users' data;

c) Defendant failed to enforce or ensure compliance with their own privacy promises to consumers by, for example, failing to establish or enforce any internal

privacy compliance programs, protocols, or policies, such as relating to data sharing and third-party SDKs;

d) Defendant failed to develop policies regarding the secure implementation of third-party SDKs, including policies that ensured that the implementation of third-party SDKs complied with Defendant's privacy promises and mobile app store policies and protected Premom users' data and privacy; and

d) Defendant failed to provide adequate privacy training for those employees responsible for incorporating and testing third-party SDKs.

47. As a result of these privacy failures, Defendant failed to encrypt or label its Custom App Events to prevent the transfer of Premom users' health information to Google and AppsFlyer.

48. In addition, as a result of these privacy failures, Defendant did not take steps to address Jiguang's and Umeng's collection of multiple mobile device identifiers of their users or investigate the purposes for which Jiguang and Umeng collected this data, as described above. Defendant failed to take reasonable measures to assess and address data security risks created by third-party SDKs incorporated into Premom. Specifically, JPush fails to encrypt adequately Premom users' sensitive information. When JPush transferred users' information to Jiguang's servers outside the United States, JPush both utilized a non-standard encryption method and included the decryption key in the transfer. As a result of these practices, any third party who acquired this data, including foreign governments or bad actors, could decrypt and access Premom users' sensitive data, including precise geolocation information and non-resettable identifiers described above.

Consumer Injury

49. As a further result of these privacy and data security failures, consumers suffered both increased risks of harm and actual harm. Among other harms:

a) Users' sensitive, device identifiers, including non-resettable identifiers, and other identifiable data were sent with inadequate encryption or similar protective measures to third parties outside the United States, subjecting this data and information to potential interception and/or seizure by bad actors and foreign governments;

b) Users' sensitive, non-resettable device identifiers and identifiable data were transferred to third parties, without users' knowledge or consent, for the purpose of third-party advertising. The transfer of non-resettable device identifiers and identifiable data enabled these third parties to target and track users in a way that circumvented users' operating system privacy controls, without users' knowledge or consent; and

c) Users' health information has been shared with third parties, without users' authorization. Defendant's sharing of Premom users' Custom App Events and persistent identifiers has revealed highly sensitive and private details about their users. This has led to the unauthorized disclosure of facts about individuals' sexual and reproductive health, parental and pregnancy status, as well as other information about an individuals' physical health conditions and status. Disclosure of this information without authorization is likely to cause Premom users stigma, embarrassment, or emotional distress, and may also affect their

ability to obtain or retain employment, housing, health insurance, disability insurance, or other services. Moreover, it has increased the risk of further unauthorized disclosures.

50. Consumers had no way of independently knowing about Defendant's privacy and data security failures and could not reasonably have avoided possible harms from such failures.

DEFENDANT VIOLATED THE HEALTH BREACH NOTIFICATION RULE

51. Congress enacted the American Recovery and Reinvestment Act of 2009, which directed the FTC to promulgate a rule requiring vendors of personal health records and related entities that collect healthcare information to provide notice to consumers and the FTC following a breach of security.

52. The FTC published a notice of proposed rulemaking on April 16, 2009 and promulgated the Rule and published supplementary information on August 17, 2009, under Section 13407 of the American Recovery and Reinvestment Act of 2009, Public Law 111-5, 123 Stat. 115 (2009). The Rule became effective on August 25, 2009, and companies became subject to FTC enforcement on February 22, 2010. Pursuant to Section 13407 of the American Recovery and Reinvestment Act of 2009, and section 18(a)(1)(B) of the FTC Act, 15 U.S.C. § 57a(a)(1)(B), a violation of the Rule constitutes an unfair or deceptive act or practice in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

53. Among other things, the Rule requires vendors of personal health records ("PHR") and PHR related entities to notify U.S. consumers and the FTC, and in some cases, the media, if they experience a breach of security.

54. The Rule defines "breach of security" to mean "with respect to unsecured PHR identifiable health information of an individual in a personal health record, acquisition of such information without the authorization of the individual." 16 C.F.R. § 318.2(a).

55. The Rule defines "personal health record" to mean "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." 16 C.F.R. § 318.2(d).

56. The Rule defines "PHR identifiable health information" to mean "'individually identifiable health information,' as defined in section 1171(6) of the Social Security Act (42 U.S.C. 1320d(6)), and, with respect to an individual, information: (1) [t]hat is provided by or on behalf of the individual; and (2) [t]hat identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual." 16 C.F.R. § 318.2(e).

57. The Rule defines "vendor of personal health records" to mean "an entity, other than a HIPAA-covered entity or an entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity, that offers or maintains a personal health record." 16 C.F.R. § 318.2(j).

58. The Rule defines "unsecured" to mean with respect to PHR identifiable information, such information "that is not protected through the use of a technology or methodology specified by the Secretary of Health and Human Services in guidance issued under section 13402(h)(2) of the American Reinvestment and Recovery Act of 2009. This guidance specifies that PHR identifiable information is protected when such information is "rendered

unusable, unreadable, or indecipherable to unauthorized individuals" using technology such as encryption.

59. Defendant is a vendor of personal health records under the Rule. Defendant offers Premom, which is a personal health record because Premom collects and receives PHR identifiable health information from multiple sources. As described in Paragraphs 14 to 17, Premom users input health information into the Premom app. Among other health information, a Premom user can upload a picture of an ovulation test, which Premom then analyzes to determine whether the user is ovulating. Premom also collects users' health and non-health information from Bluetooth thermometers or third-party apps; for instance, a user can import from Apple Health her temperature and the date and time the temperature was taken. Moreover, as described in Paragraphs 13 to 17, Premom users manage and control the PHR identifiable health information held in the Premom app. Each individual Premom user decides whether to input health information into Premom and how many of Premom's functions and services she will utilize.

60. In numerous instances, beginning in at least 2017, Defendant, as "a vendor of personal health records," experienced "breaches of security" of more than 500 consumers' unsecured PHR identifiable health information through the disclosure, and subsequent acquisition of Custom App Event titles relaying such information, by third parties such as Google and AppsFlyer, without the authorization of Premom users. This PHR identifiable health information was unsecured. This information was transferred to third parties such as Google and AppsFlyer without the use of encryption or other means to render it unusable,

unreadable, or indecipherable to unauthorized individuals because this information was sent as Custom App Event titles in plain text, as described in Paragraphs 26 to 28 above.

61. Based on the facts and violations of law alleged in this Complaint, the FTC has reason to believe that Defendant is violating or is about to violate laws enforced by the Commission because, among other things, Defendant has shared PHR identifiable health information with third parties without obtaining Premom users' authorization. Defendant's violation of the Health Breach Notification Rule is ongoing. Defendant has not notified users, in accordance with the notification provisions of the Health Breach Notification Rule, that it breached the security of Premom users' PHR identifiable health information through Premom's unauthorized disclosures to Google and AppsFlyer.

62. Section 5(m)(1)(A) of the FTC Act, 15 U.S.C. § 45(m)(1)(A), as modified by Section 4 of the Federal Civil Penalties Inflation Adjustment Act of 1990, 28 U.S.C. § 2461, the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015, Public Law 114-74, sec. 701, 129 Stat. 599 (2015), and Section 1.98(d) of the FTC's Rules of Practice, 16 C.F.R. § 1.98(d), authorizes this Court to award monetary civil penalties of not more than $46,517 for each knowing violation of the Rule.

63. Defendant has violated the Rule with the knowledge required by Section 5(m)(1)(A) of the FTC Act, 15 U.S.C. § 45(m)(1)(A).

VIOLATIONS OF THE FTC ACT

64. Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibits "unfair or deceptive acts or practices in or affecting commerce."

65. Misrepresentations or deceptive omissions of material fact constitute deceptive acts or practices prohibited by Section 5(a) of the FTC Act.

66. Acts or practices are unfair under Section 5 of the FTC Act if they cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45(n).

Count I

Privacy Misrepresentation – Disclosures of Health Information

67. In numerous instances, as alleged in Paragraphs 19 and 20, Defendant has represented, directly or indirectly, expressly or by implication, that it would not disclose, without consumers' knowledge or consent, their health information to third parties, that AppsFlyer would not receive consumers' health information, and that third party services would not receive consumers' health information unless the consumer shares the health information directly to them.

68. In truth and fact, in numerous instances in which Defendant made the representations set forth in Paragraph 67, Defendant did disclose consumers' health information to AppsFlyer and Google as set forth in Paragraphs 4 and 25 to 31.

69. Therefore, Defendant's representations as set forth in Paragraph 67 are false or misleading and constitute a deceptive act or practice in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

Count II

Privacy Misrepresentation – Sharing Data with Third Parties

70. In numerous instances, as alleged in Paragraph 21, Defendant represented, directly or indirectly, expressly or by implication, to consumers that Defendant shared *only* non-identifiable information to third parties and that these third parties tracked users *only* by IP address.

71. In truth and fact, in numerous instances in which Defendant made the representations as set forth in Paragraph 70, Defendant did disclose identifiable information to third parties, which tracked users by means other than IP address. Namely, Defendant conveyed to third parties (1) social media account information through the U-Share SDK; (2) device identifiers that could be used to identify users; and/or (3) precise geolocation information as set forth in Paragraphs 5 to 6 and 33 to 41.

72. Therefore, Defendant's representations as set forth in Paragraph 70 are false and misleading and constitute a deceptive act or practice in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

Count III

Deceptive Failure to Disclose – Sharing Geolocation Information with Third Parties

73. In numerous instances, as alleged in Paragraph 22, Defendant represented, directly or indirectly, expressly or by implication, to consumers that consumers needed to turn on location sharing so that Premom could locate consumers' Bluetooth thermometers.

74. In numerous instances in which Defendant made the representations as set forth in Paragraph 73, Defendant failed to disclose, or failed to disclose adequately, that Defendant conveyed users' geolocation information to Umeng and Jiguang, which Umeng and Jiguang

could use and transfer for their own purposes, including third-party advertising. This additional information would be material to consumers in their decision to use Defendant's services.

75. In light of the representations set forth in Paragraph 73, Defendant's failure to disclose the material information described in Paragraph 74 constitutes a deceptive act or practice in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

Count IV

Privacy Misrepresentation – Third Parties' Use of Shared Data

76. In numerous instances, as alleged in Paragraph 23, Defendant represented, directly or indirectly, expressly or by implication, to consumers that Defendant would not use Premom users' information for any purpose other than those purposes outlined in Defendant's privacy policies and terms of service.

77. As alleged in Paragraph 23, Defendant further represented, directly or indirectly, expressly or by implication, to consumers that their data would be used and shared for Defendant's own analytics and advertising.

78. In truth and fact, in numerous instances in which Defendant made the representations as set forth in Paragraphs 76 and 77, Defendant's representations were false or misleading. These representations were false or misleading because Defendant incorporated U-Share and JPush into Premom. By incorporating U-Share and JPush, Defendant conveyed users' personal information to Umeng and Jiguang, which Umeng and Jiguang could use for their own purposes, such as third-party advertising as set forth in Paragraph 40.

79. Therefore, Defendant's representations as set forth in Paragraphs 76 and 77 are false and constitute a deceptive act or practice in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

Count V

Deceptive Failure to Disclose – Third Parties' Use of Shared Data

80. In numerous instances as alleged in Paragraph 23, Defendant represented, directly or indirectly, expressly or by implication, to consumers that their data would be used and shared for Defendant's own analytics and advertising.

81. In numerous instances in which Defendant made the representations set forth in Paragraphs 80, Defendant failed to disclose, or failed to disclose adequately, that by incorporating U-Share and JPush into Premom, Defendant conveyed users' personal information to Umeng and Jiguang, which Umeng and Jiguang could use and transfer for their own purposes, such as third-party advertising, as set forth in Paragraph 41. This additional information would be material to consumers in their decision to use Defendant's services.

82. In light of the representations set forth in Paragraphs 80, Defendant's failure to disclose the material information described in Paragraph 81 constitutes a deceptive act or practice in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

Count VI

Unfair Privacy and Data Security Practices

83. In numerous instances as alleged in Paragraphs 46 to 48, Defendant failed to take reasonable measures to assess and address the privacy and data security risks created by third-party software it chose to incorporate into Premom.

84. As described in Paragraphs 48 to 50, Defendant's actions caused or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition.

85. Therefore, Defendant's acts or practices as set forth in Paragraph 83 constitute unfair acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

Count VII

Unfair Sharing of Health Information for Advertising Purposes Without Affirmative Express Consent

86. In numerous instances as alleged in Paragraphs 26 to 29, 47, and 48, Defendant failed to encrypt or label Premom users' Custom App Events to prevent the transfer of users' personal health information to Google and AppsFlyer. Because Defendant failed to encrypt or label Premom users' Custom App Events, Defendant transferred their users' health information to third parties without users' knowledge, and without providing users notice or obtaining users' affirmative express consent.

87. As described in Paragraphs 49 and 50, Defendant's actions caused or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition.

88. Therefore, Defendant's acts or practices as set forth in Paragraph 86 constitute an unfair act or practice in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

Count VIII

VIOLATION OF THE HEALTH BREACH NOTIFICATION RULE

16 C.F.R. § 318

89. Defendant is a "vendor of personal health records," as defined by Sections 318.2(d), 318.2(e), and 318.2(j) of the HBNR. 16 CFR. §§ 318.2(d), (e), (j). Defendant is an entity, other than a HIPAA-covered entity, or an entity, to the extent that it engages in activities as a business associated of a HIPAA-covered entity, that maintains "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." As described in Paragraphs 14 to 17, Premom draws health information from multiple sources. For instance, it allows users to input their own health information into Premom. Among other health information, a Premom user can upload a picture of an ovulation test, which Premom then analyzes to determine whether the user is ovulating. Premom also collects users' health and non-health information from Bluetooth thermometers or third-party apps; for instance, a user can import from Apple Health her temperature and the date and time the temperature was taken. The information is managed, shared, or controlled by or primarily for the user. As described in Paragraphs 13 to 17, Premom allows users to manage and control the PHR identifiable health information held in the Premom app, and allows users to track their ovulation, menstruation, and other health information.

90. In numerous instances, beginning in at least 2017, Defendant, as "a vendor of personal health records," experienced "breaches of security" of more than 500 consumers' unsecured PHR identifiable health information through the disclosure, and subsequent acquisition of Custom App Event titles relaying such information, by third parties such as Google and AppsFlyer, without the authorization of Premom users. This PHR identifiable health information was unsecured. This information was transferred to third parties such as Google and AppsFlyer without the use of encryption or other means to render it unusable,

unreadable, or indecipherable to unauthorized individuals because this information was sent as Custom App Event titles in plain text, as described in Paragraphs 26 to 28 above.

91. Defendant has failed to provide the required notifications, as prescribed by the HBNR, to (1) individuals whose unsecured PHR identifiable health information was acquired by an unauthorized person; (2) to the Federal Trade Commission; or (3) to media outlets. 16 C.F.R. §§ 318.3–6.

92. Pursuant to Section 13407(e) of the 2009 Recovery Act, and Section 318.7 of the HBNR, a violation of the HBNR constitutes an unfair or deceptive act or practice in or affecting commerce, in violation of Section 5(a) of the FTC Act. 42 U.S.C. § 17937(e); 16 CFR § 318.7; 15 U.S.C. §§ 45(a), 57a(d)(3).

93. Therefore, Defendant's acts or practices as set forth in Paragraphs 89 to 91 are deceptive and unfair acts or practices that violate Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

CONSUMER INJURY

94. Consumers are suffering, have suffered, and will continue to suffer substantial injury as a result of Defendant's violations of the FTC Act. Absent injunctive relief by this Court, Defendant is likely to continue to injure consumers and harm the public interest. Moreover, Defendant's continued failure to notify consumers of its unauthorized disclosures, pursuant to the Health Breach Notification Rule, further harms users by depriving them of notice and an opportunity to mitigate the unauthorized disclosures, and any past, present, or future harm that may occur.

PRAYER FOR RELIEF

Wherefore, Plaintiff requests that the Court:

A. Enter a permanent injunction to prevent future violations of the FTC Act and the Health Breach Notification Rule by Defendant;

B. Award Plaintiff monetary civil penalties from Defendant for each violation of the Health Breach Notification Rule alleged in this Complaint; and

C. Award any additional relief as the Court determines to be just and proper.

Dated: May 17, 2023

OF COUNSEL

FOR THE FEDERAL TRADE COMMISSION:

TIFFANY GEORGE
Acting Assistant Director
Division of Privacy and Identity Protection

DAVID WALKO
Attorney
Division of Privacy and Identity Protection
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
(202) 326-2880
(202) 326-3062 (fax)

RONNIE SOLOMON
Attorney
Division of Privacy and Identity Protection
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
(202) 326-2098
(202) 326-3062 (fax)

FOR PLAINTIFF THE UNITED STATES OF AMERICA:

BRIAN M. BOYNTON
Principal Deputy Assistant Attorney General
Civil Division

ARUN G. RAO
Deputy Assistant Attorney General

AMANDA N. LISKAMM
Director

LISA K. HSIAO
Assistant Director

/s/ *Rachel E. Baron*
RACHEL E. BARON
Trial Attorney
Consumer Protection Branch
U.S. Department of Justice
Civil Division
450 Fifth Street NW
Washington, D.C. 20530
(202) 598-7719