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. §§

4.

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.

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

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(')Tj0.33 0 Td( )Tj[(j0.02e)-6 (r)3 (s)v4 (in-2 (e)4-1 (s)-1 (t)-2 (it)-2 (s)-1 (de)4 ((i)-2 (c)4 de)4 (')3 (s)-

32. Fiaell,d antrfresee(t)-2 ((a)4 (t)-2 (('

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 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.

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 tk—l lo (w)2 (o)-10 ion usd d c

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 identifiert (t)-6 (y)-4 T(om)-2 (e)4(a)6 (p)(he)4 (s)- esom6 (hi)-n (r)-1 (t)-6 thout pur canr puTf3 0 T8

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

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-

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

65. Misrepresentations or deceptive omissions of material fact constitut

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.

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’ affw 13.49 -24 (or)3 Twt(nc)-6 (.)]TJ0 Tce7þ ansefarsnd A

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

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

FOR PLAINTIFF THE UNITED STATES OF AMERICA:

BRIAN M. BOYNTON
Principal Deputy Assistant Attorney General
Civil Division

ARUN G. RAO
Deputy Assistant Attorneo()Y.0 Tw 0.81 0 Tdsion of Privac