

**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK**

MARTINE DAVIS, individually and on behalf of
all others similarly situated,

Plaintiff,

v.

LIFERX.MD, INC.,

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Martine Davis (“Plaintiff”), individually and on behalf of all others similarly situated, by and through her attorneys, makes the following allegations pursuant to the investigation of her counsel and based upon information and belief, except as to allegations specifically pertaining to herself, which are based on personal knowledge.

NATURE OF ACTION

1. This is a class action lawsuit brought on behalf of all persons who have visited the website liferx.md (the “Website”) and booked an appointment for Glucagon-like peptide-1 (“GLP-1”) weight loss medication.

2. LifeRx.md, Inc. (“Defendant”) is an online provider of GLP-1 weight loss medication.

3. When consumers visit the Website, they must book an appointment to determine whether they qualify for Defendant’s weight loss medication. Unbeknownst to Plaintiff and members of the putative class, and contrary to Defendant’s own representations, Defendant discloses their personally identifiable information to third parties for targeted advertising purposes. Plaintiff therefore brings this action for legal and equitable remedies resulting from Defendant’s illegal actions.

THE PARTIES

4. At all relevant times Plaintiff Martine Davis was a resident of New York, New York. In September 2023, Plaintiff booked an appointment for GLP-1 medication through Defendant's Website. When booking her appointment, Plaintiff provided Defendant with her personal information, including her name, email address, and phone number. Unbeknownst to Plaintiff, Defendant disclosed her personal information—as well as her attempt to seek weight loss medication—to third parties for targeted advertising purposes. After booking an appointment on Defendant's Website, Plaintiff began receiving targeted advertisements for similar products and services. Plaintiff would not have booked an appointment on Defendant's Website if she knew Defendant was violating her privacy by sharing her personal information with unknown third parties.

5. LifeRx.md, Inc. is a Delaware corporation with its principal place of business in Cherry Hill, New Jersey. Defendant develops, owns, and operates liferx.md, which is used by consumers throughout New York to book appointments for weight loss medication.

JURISDICTION AND VENUE

6. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A) as modified by the Class Action Fairness Act of 2005, because at least one member of the Class, as defined below, is a citizen of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds \$5,000,000 exclusive of interests and costs.

7. This Court has personal jurisdiction over Defendant because Defendant conducts substantial business within this District.

8. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because a substantial part of the events giving rise to this claim occurred in this District.

FACTUAL ALLEGATIONS COMMON TO ALL CLAIMS

A. Health-Related Information is Sensitive and Confidential

9. Defendant assisted X Corp. (f/k/a Twitter, Inc.), Pinterest, Inc., Microsoft Corporation, Google, LLC, and Taboola, Inc. with intercepting information that is sensitive, confidential, and personally identifiable.

10. Defendant is an online provider of GLP-1 weight loss medication.

11. Under federal law, a healthcare provider may not disclose personally identifiable information (“PII”) or protected health information (“PHI”) without the patient’s express written authorization.¹ In this case, PHI includes but is not limited to information pertaining to medical prescriptions relating to GLP-1 weight loss medication.

12. The United States Department of Health and Human Services (“HHS”) has established a national standard, known as the HIPAA Privacy Rule, to explain the duties healthcare providers owe to their patients. “The Rule requires appropriate safeguards to protect the privacy of [PHI] and sets limits and conditions on the uses and disclosures that may be made of such information without an individual’s authorization.”²

13. A healthcare provider violates the HIPAA Privacy Rule if it knowingly and in violation of 42 U.S.C. §§ 1320d-d9 (“Part C”): “(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual.”³

¹ HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502, 165.508(a), 164.514(b)(2)(i).

² U.S. Dept. of Health and Human Services, <https://www.hhs.gov/hipaa/for-professionals/privacy/index.html>.

³ 42 U.S.C. § 1320d-6.

14. The statute states that an entity “shall be considered to have obtained or disclosed individually identifiable health information in violation of [Part C] if the information is maintained by a covered entity...and the individual obtained or disclosed such information without authorization.” *Id.*

15. The criminal and civil penalties imposed by 42 U.S.C. § 1320d-6 apply directly to Defendant when it is knowingly disclosing individually identifiable health information relating to its patients.

16. Defendant further failed to comply with other HIPAA safeguard regulations as follows:

- a. Failing to ensure the confidentiality and integrity of electronic PHI that LifeRx created, received, maintained and transmitted in violation of 45 C.F.R. Section 164.306(a)(1);
- b. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. Section 164.308(a)(1);
- c. Failing to identify and respond to suspected or known security incidents and mitigate harmful effects of security incidents known to LifeRx in violation of 45 C.F.R. Section 164.308(a)(6)(ii);
- d. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. Section 306(a)(2);
- e. Failing to protect against reasonably anticipated uses of disclosures of electronic PHI not permitted under privacy rules pertaining to individually

identifiable health information in violation of 45 C.F.R. Section 164.306(a)(3); and

- f. Failing to design, implement and enforce policies and procedures that would establish physical and administrative safeguards to reasonably safeguard PHI in violation of 45 C.F.R. Section 164.530(c).

17. Health care organizations regulated under HIPAA, like Defendant, may use third-party tracking tools in a limited way to perform analysis on data key to operations. They are not permitted, however, to use these tools in a way that may expose patients' PHI to vendors (as shown below in Figures 3 through 7). As explained by a statement published by the HHS:

Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. **For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.**⁴

18. The Bulletin discusses the types of harm that disclosure may cause to the patient:

An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment. While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, **because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule.**⁵

⁴ HHS.gov, USE OF ONLINE TRACKING TECHNOLOGIES BY HIPAA COVERED ENTITIES AND BUSINESS ASSOCIATES (THE "BULLETIN") (EMPHASIS ADDED), <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html>.

⁵ *Id.* (emphasis added).

19. Plaintiff and Class Members face exactly the risks about which the government expresses concern. Defendant's unlawful conduct resulted in third parties intercepting information regarding Plaintiff and Class Members scheduling consultations on the Website.

20. The Bulletin goes on to make clear how broad the government's view of protected information is. It explains:

This information might include an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, medical device IDs, **or any unique identifying code.**⁶

21. Crucially, that paragraph in the government's Bulletin continues:

All such [individually identifiable health information ("IIHI")] collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services. This is because, when a regulated entity collects the individual's IIHI through its website or mobile app, the information connects the individual to the regulated entity (i.e., it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care.⁷

22. Then, in July 2022, the Federal Trade Commission ("FTC") and the Department of Health and Human Services ("HHS") issued a joint press release warning regulated entities about the privacy and security risks arising from the use of online tracking technologies:

The Federal Trade Commission and the U.S. Department of Health and Human Services' Office for Civil Rights (OCR) are cautioning hospitals and telehealth providers [regulated entities] about the privacy and security risks related to the use of online tracking technologies integrated into their websites or mobile apps that may be impermissibly disclosing consumers' sensitive personal health data to third parties.

"When consumers visit a hospital's [regulated entity's] website or seek telehealth services, they should not have to worry that their most private and sensitive health

⁶ *Id.* (emphasis added).

⁷ *Id.*

information may be disclosed to advertisers and other unnamed, hidden third parties,” said Samuel Levine, Director of the FTC’s Bureau of Consumer Protection. “The FTC is again serving notice that companies need to exercise extreme caution when using online tracking technologies and that we will continue doing everything in our powers to protect consumers’ health information from potential misuse and exploitation.”

“Although online tracking technologies can be used for beneficial purposes, patients and others should not have to sacrifice the privacy of their health information when using a hospital’s [regulated entity’s] website,” said Melanie Fontes Rainer, OCR Director. “OCR continues to be concerned about impermissible disclosures of health information to third parties and will use all of its resources to address this issue.”

The two agencies sent the joint letter to approximately 130 [regulated entities] hospital systems and telehealth providers to alert them about the risks and concerns about the use of technologies, such as the Meta/Facebook pixel and Google Analytics, that can track a user’s online activities. These tracking technologies gather identifiable information about users, usually without their knowledge and in ways that are hard for users to avoid, as users interact with a website or mobile app.

In their letter, both agencies reiterated the risks posed by the unauthorized disclosure of an individual’s personal health information to third parties. For example, the disclosure of such information could reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, and where an individual seeks medical treatment.⁸

23. Therefore, Defendant’s conduct, as described more thoroughly below, is directly contrary to federal law and the clear pronouncements by the FTC and HHS.

⁸ Federal Trade Commission, *FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies*, July 20, 2023, <https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking>.

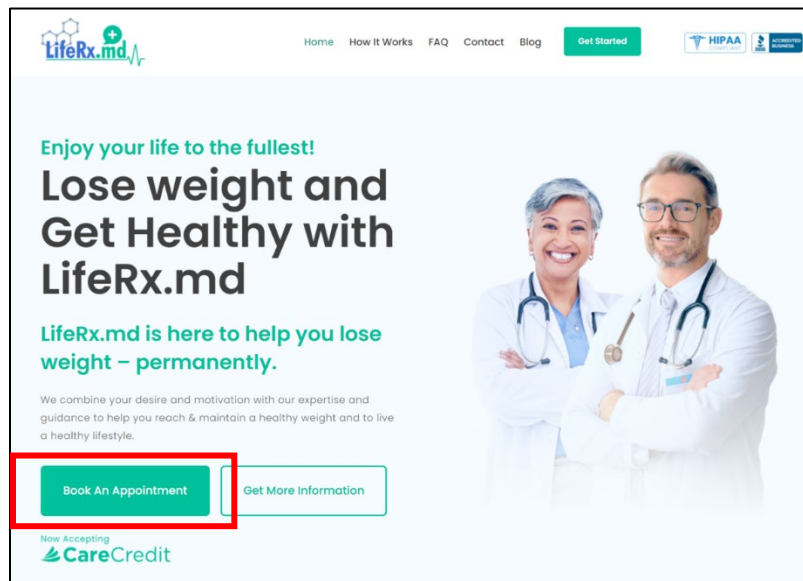
B. Defendant Violates the Privacy Rights of its Customers

24. GLP-1 medications, such as Ozempic, are surging in popularity. These medications are expected to reach \$150 billion in sales within the next ten years.⁹

25. Defendant requires prospective customers to book appointments through its Website to determine whether they qualify for these weight loss medications. To book an appointment, Defendant requests personal information from consumers, such as their name, email address, and phone number. Unbeknownst to consumers, and despite Defendants explicit representations to the contrary, Defendant shares this information with third parties for targeted advertising purposes.

26. To start, users click “Book An Appointment.”

Figure 1:



⁹ Beasley, Deena, *Weight-loss drug forecasts jump to \$150 billion as supply grows*, Reuters (May 28, 2024).

27. When users click “Book An Appointment,” Defendant requests personal information to connect them with one of its agents.

Figure 2:

LifeRx.md

Book an Appointment

Complete the form below to be connected with an agent and schedule an appointment.

Name

Email

Mobile Phone

☐ I agree with LifeRx.md's Terms and Conditions and Privacy Policy

☐ I want to receive phone calls, appointment updates and marketing messages via SMS.

BOOK AN APPOINTMENT

We do not sell or share your information with anyone.

[Privacy Policy](#) | [Terms of Service](#)

28. As shown in Figure 2, Defendant expressly warrants to consumers that it “do[es] not sell or share your information with anyone.”

29. However, Defendant shares consumers’ personal information with several advertising partners, including, but not necessarily limited to, X Corp. (f/k/a Twitter, Inc.), Pinterest, Inc., Microsoft Corporation, Google, LLC, and Taboola, Inc. The information shared by Defendant allows these advertising partners to know the identities of specific individuals interested in purchasing GLP-1 medications. This allows these companies, including Defendant, to profit from this information for targeted advertising purposes.

30. For example, after a consumer clicks “BOOK AN APPOINTMENT,” Defendant sends their name, email address, and phone number to its advertising partners, as shown in Figures 3-7.

Figure 3:

```

"status": "COMPLETE",
"method": "GET",
"protocolVersion": "HTTP/2.0",
"scheme": "https",
"host": "bat.bing.com",
"actualPort": 443,
"path": "/action/0",
"query":
  "ti=97130562
  Ver=2
  mid=a2aad83b-7478-41f2-84e7-ed643d5caa73
  sid=2f820da038bd11efa318b9d955d3989a
  vid=2f8249a038bd11efaf138d04d2fbc56e
  vids=0
  msclkid=N
  uach=pv=15.0.0
  pi=918639831
  lg=en-US
  sw=3072
  sh=1728
  sc=24
  tl=Thank you - LifeRx.md
  p=https://liferx.md/thank-you/?om_name=Thomas Anderson
  om_email=thommy5431@yahoo.com
  om_phone=7863486767

```

Figure 4:

```

Endpoint: https://googleads.g.doubleclick.net/pagead/viewthroughconversion/11480207165/
Date: Tue Jul 02 17:52:03 EDT 2024

Data:
random 38482850
cv 11
fst 1719957122995
bg ffffff
guid ON
async 1
gtm 45be4710v9176727086z89176257312za201zb9176257312
gcd 13l3l3l3l1
dma 0
tag_exp 0
u_w 3072
u_h 1728
url https://liferx.md/thank-you/?
  om_name=Thomas Anderson
  om_email=thommy5431@yahoo.com
  om_phone=7863486767

```

Figure 5:

```

Endpoint: https://analytics.twitter.com/1/i/adsct
Date: Tue Jul 02 17:52:03 EDT 2024

Data:
bci 4
eci 3
event {}
event_id 9b855003-31fe-4888-acb8-2591291f73eb
integration advertiser
p_id Twitter
p_user_id 0
pl_id 03c04e70-3eba-4782-b733-f9bffe32d584
tw_document_href https://liferx.md/thank-you/?
  om_name=Thomas Anderson
  om_email=thommy5431@yahoo.com
  om_phone=7863486767

```

Figure 6:

```

Endpoint: https://ct.pinterest.com/v3/
Date: Tue Jul 02 17:52:03 EDT 2024

Data:
event lead
ed {"event_id":"eventId0001"
"lead_type":"Newsletter"}
tid 2613652177278
cb 1719957123053
dep 5
EVENT_TAGS_ABSENT
pd {"em":"24aba99b2defbb47ee981b4200313f61f3ae31541d8717bdac1e463c838939b0"
"pin_unauth":"dWlkPVIUSXdORGhtWWprdE9EYzBZUzAwWXPfNEXSm1NVFI0TldOaU56UmhaRE16T1RWaA"}
ad {"loc":"https://liferx.md/thank-you/?
om_name=Thomas Anderson
om_email=thommy5431@yahoo.com
om_phone=7863486767

```

Figure 7:

```

Endpoint: https://trc.taboola.com/589374/trc/3/json
Date: Tue Jul 02 17:52:02 EDT 2024

Data:
tim 1719957122884
data [{"id":279
"ti":"thank-you"
"it":"video"
"sd":{"v2_09cb589a00937644ddbffa100b3aec3_b6ab163c-9cb9-46f1-8e7f-d9edc2ec4b23-tuctce22189_1719957066_1719957095_CAwQ_oBhGJKNuquHMIADKAMw4QE4kaQQQPG-Dkivy9kDUJAEWABgAGji49WDy7fg_rkBcAE"
"ui":"b6ab163c-9cb9-46f1-8e7f-d9edc2ec4b23-tuctce22189"
"vi":1719957122881
"cv":"20240626-2-RELEASE"
"ui":"default"
"u":"https://liferx.md/thank-you/"
"e":"https://liferx.md/"
"cb":"TFASC.trkCallback"
"qs":"?
om_name=Thomas Anderson
om_email=thommy5431@yahoo.com
om_phone=7863486767

```

31. As shown above, Plaintiff's communications with Defendant were disclosed by Defendant to these third parties and/or intercepted in transit by the third parties, in real time, via detailed URLs, which contain the medically sensitive information and personally identifiable information entered into the Website.

32. When consumers share their personal information with medical professionals, they expect this information to be kept confidential. Moreover, when consumers seek a specific medical consultation and/or treatment from medical professionals, they also expect this highly sensitive information to be kept confidential.

33. Defendant lulls consumers into a false sense of security by representing that its Website is “HIPAA compliant” and that it will “not sell or share your information with anyone.” But that is not true because Defendant shares personal information about consumers with third parties such as X Corp., Pinterest, and Microsoft.

34. Defendant knows these representations are crucial due to the competitive market for GLP-1 medications. If consumers knew that Defendant was sharing their personal information for targeted advertising purposes, they would go to one of its competitors. Through the above-listed third parties’ tracking services, which Defendant used via the software code installed, integrated and embedded into the Website, Defendants disclosed consumers’ identities and sensitive medical information.

35. By installing, integrating and embedding the above-listed tracking technologies into the Website, and by directing such installation, integration and embedding, Defendant aided and conspired with the third parties and others to allow those third-party entities to contemporaneously and surreptitiously intercept the Website communications of Defendant’s customers without customer consent.

36. Defendant engages in this deceptive conduct for its own profit at the expense of its customers. Such disclosures are an invasion of privacy, lead to harassing targeted advertising, and violates New York and federal law.

CLASS ACTION ALLEGATIONS

37. Plaintiff brings this action on behalf of all persons in the United States who booked an appointment on liferx.md (the “Class”).

38. Plaintiff also brings this action on behalf of all persons in New York who booked an appointment on liferx.md (the “Subclass”).

39. Excluded from the Class is Defendant, the officers and directors of the Defendant at all relevant times, members of their immediate families and their legal representatives, heirs, successors or assigns and any entity in which either Defendant has or had a controlling interest.

40. Plaintiff is a member of the Classes she seeks to represent.

41. The Class is so numerous that joinder of all members is impractical. Although Plaintiff does not yet know the exact size of the Class, Defendant claims to have “Over 50,000+ Weight Loss Patients.”¹⁰

42. The Class is ascertainable because the Class members can be identified by objective criteria – all individuals who booked an appointment on liferx.md. Individual notice can be provided to Class members “who can be identified through reasonable effort.” Fed. R. Civ. P. 23(c)(2)(B).

43. There are numerous questions of law and fact common to the Class, which predominate over any individual actions or issues, including but not limited to:

- A. Whether Defendant gave the Class members a reasonable expectation of privacy that their information was not being shared with third parties;
- B. Whether Defendant’s disclosure of information constitutes a violation of the claims asserted;
- C. Whether Plaintiff and Class members are entitled to declaratory and/or injunctive relief to enjoin the unlawful conduct alleged herein; and
- D. Whether Plaintiff and Class members have sustained damages as a result of Defendant’s conduct and if so, what is the appropriate measure of damages or restitution.

¹⁰ <https://liferx.md/>

44. Plaintiff's claims are typical of the claims of the members of the Class, as all members are similarly affected by Defendant's wrongful conduct. Plaintiff has no interests antagonistic to the interests of the other members of the Class. Plaintiff and all members of the Class have sustained economic injury arising out of Defendant's violations of common and statutory law as alleged herein.

45. Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the Class members she seeks to represent, she has retained counsel competent and experienced in prosecuting class actions, and she intends to prosecute this action vigorously. The interests of Class members will be fairly and adequately protected by Plaintiff and her counsel.

46. The class mechanism is superior to other available means for the fair and efficient adjudication of the claims of Plaintiff and Class members. Each individual Class member may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by the complex legal and factual issues of this case. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability issues will ensure that all claims are consistently adjudicated.

47. Plaintiff reserves the right to revise the foregoing class allegations and definitions based on facts learned and legal developments following additional investigation, discovery, or otherwise.

CAUSES OF ACTION

COUNT I

Violation of the Electronic Communications Privacy Act 18 U.S.C. § 2511(1), *et seq.*

48. Plaintiff incorporates by reference the allegations contained in the paragraphs above as if fully set forth herein.

49. Plaintiff brings this claim on behalf of herself and members of the nationwide Class.

50. The Electronic Communications Privacy Act (“ECPA”) prohibits the intentional interception of the content of any electronic communication. 18 U.S.C. § 2511.

51. The ECPA protects both sending and the receipt of communications.

52. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

53. The transmission of Plaintiff’s PII and PHI to Defendant’s Website qualify as a “communication” under the ECPA’s definition of 18 U.S.C. § 2510(12).

54. The transmission of PII and PHI between Plaintiff and Class Members and Defendant’s Website with which they chose to exchange communications are “transfer[s] of signs, signals, writing,...data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate

commerce” and are therefore “electronic communications” within the meaning of 18 U.S.C. § 2510(12).

55. The ECPA defines “contents,” when used with respect to electronic communications, to “include[] any information concerning the substance, purport, or meaning of that communication.” 18 U.S.C. 18 U.S.C. § 2510(8).

56. The ECPA defines an interception as the “acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” 18 U.S.C. § 2510(4).

57. The ECPA defines “electronic, mechanical, or other device,” as “any device...which can be used to intercept a[n]...electronic communication[.]” 18 U.S.C. § 2510(5).

58. The following instruments constitute “devices” within the meaning of the ECPA:

- a. The computer codes and programs Defendant and third parties used to track Plaintiff and Class Members communications while they were navigating the Website;
- b. Plaintiff’s and Class Members’ browsers;
- c. Plaintiff’s and Class Members’ mobile devices;
- d. Defendant and X Corp., Pinterest, Inc., Microsoft Corporation, Google, LLC, and Taboola, Inc.’s web and ad servers;
- e. The plan Defendant and the above-listed third parties carried out to effectuate the tracking and interception of Plaintiff’s and Class Members’ communications while they were using a web browser to navigate the Website.

59. Plaintiff and Class Members' interactions with Defendant's Website are electronic communications under the ECPA.

60. By utilizing and embedding the tracking technology provided by X Corp., Pinterest, Inc., Microsoft Corporation, Google, LLC, and Taboola, Inc. on its Website, Defendant intentionally intercepted, endeavored to intercept, and/or procured another person to intercept, the electronic communications of Plaintiff and Class Members in violation of 18 U.S.C. § 2511(1)(a).

61. Specifically, Defendant intercepted—in real time—Plaintiff's and Class Members' electronic communications via the tracking technology provided by X Corp., Pinterest, Inc., Microsoft Corporation, Google, LLC, and Taboola, Inc. on its Website, which tracked, stored and unlawfully disclosed Plaintiff's and Class Members' PII and PHI to third parties, such as X Corp., Pinterest, Inc., Microsoft Corporation, Google, LLC, and Taboola, Inc.

62. Defendant intercepted communications that include, but are not necessarily limited to, communications to/from Plaintiff and Class Members regarding PII and PHI, including their identities and medical prescription information. This confidential information is then monetized for targeted advertising purposes, among other things.

63. By intentionally disclosing or endeavoring to disclose Plaintiff's and Class Members' electronic communications to affiliates and other third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

64. By intentionally using, or endeavoring to use, the contents of Plaintiff's and Class Members' electronic communications, while knowing or having reason to know that the

information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

65. Defendant intentionally intercepted the contents of Plaintiff's and Class Members' electronic communications for the purpose of committing a criminal or tortious act in violation of the Constitution or laws of the United States or of any state, namely, invasion of privacy, among others.

66. The party exception in 18 U.S.C. § 2511(2)(d) does not permit a party that intercepts or causes interception to escape liability if the communication is intercepted for the purpose of committing any tortious or criminal act in violation of the Constitution or laws of the United States or of any State. Here, as alleged above, Defendant violated a provision of the Health Insurance Portability and Accountability Act, specifically 42 U.S.C. § 1320d-6(a)(3). This provision imposes a criminal penalty for knowingly disclosing individually identifiable health information ("IIHI") to a third party. HIPAA defines IIHI as:

any information, including demographic information collected from an individual, that—(A) is created or received by a health care provider ... (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.¹¹

67. Plaintiff's information that Defendant disclosed to X Corp., Pinterest, Inc., Microsoft Corporation, Google, LLC, and Taboola, Inc. qualifies as IIHI, and Defendant violated Plaintiff's and Class Members' expectations of privacy. Such conduct constitutes tortious and/or criminal conduct through a violation of 42 U.S.C. § 1320d-6. Defendant used the electronic communications to increase its profit margins. Defendant specifically used the tracking

¹¹ 42 U.S.C. § 1320d-6.

technology provided by X Corp., Pinterest, Inc., Microsoft Corporation, Google, LLC, and Taboola, Inc. to track and utilize Plaintiff's and Class Members' PII and PHI for financial gain.

68. Defendant was not acting under the color of law to intercept Plaintiff's and Class Members' wire or electronic communications.

69. Plaintiff and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiff's and Class Members' privacy. Plaintiff and Class Members, all of whom are patients of Defendant, had a reasonable expectation that Defendant would not redirect their communications to X Corp., Pinterest, Inc., Microsoft Corporation, Google, LLC, and Taboola, Inc. without their knowledge or consent.

70. The foregoing acts and omission therefore constitute numerous violations of 18 U.S.C. § 2511(1), *et seq.*

71. As a result of each and every violation thereof, on behalf of herself and the Class, Plaintiff seeks statutory damages of \$10,000 or \$100 per day for each violation of 18 U.S.C. § 2510, *et seq.* under 18 U.S.C. § 2520.

COUNT II
VIOLATION OF NEW YORK GENERAL BUSINESS LAW § 349

72. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein.

73. Plaintiff brings this claim individually and on behalf of the members of the Subclass.

74. New York's General Business Law § 349 prohibits deceptive and misleading business practices.

75. In its sale of weight loss medications throughout the State of New York, Defendant conducts business and trade within the meaning and intendment of New York's General Business Law § 349.

76. Plaintiff and Subclass members are consumers who booked an appointment on Defendant's Website to receive weight loss medication for their personal use.

77. By the acts and conduct alleged herein, Defendant engaged in deceptive, unfair, and misleading acts and practices, which include, without limitation, representing that it "do[es] not sell or share your information with anyone," while then sharing its consumers' personal information with third parties. A reasonable person would understand Defendant's representation to mean that Defendant is not sharing consumers' personal information with any third party.

78. The foregoing acts and practices were directed at consumers.

79. The foregoing deceptive acts and practices are misleading in a material way because they fundamentally misrepresent how Defendant treats its consumers' personal information.

80. By reason of this conduct, Defendant engaged in deceptive conduct in violation of New York's General Business Law.

81. Defendant's actions are the direct, foreseeable, and proximate cause of the damages that Plaintiff and members of the Subclass have sustained.

82. On behalf of herself and other members of the Class, Plaintiff seeks to recover her actual damages or fifty dollars, whichever is greater, and reasonable attorneys' fees.

COUNT III
VIOLATION OF NEW YORK GENERAL BUSINESS LAW § 350

83. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein.

84. Plaintiff brings this claim individually and on behalf of the members of the Subclass.

85. Based on the foregoing, Defendant has engaged in consumer-oriented conduct that is deceptive or misleading in a material way which constitutes false advertising in violation of Section 350 of the New York General Business Law by misrepresenting that it was protecting consumers private personal information when booking an appointment on its Website.

86. The foregoing advertising was directed at consumers and was likely to mislead a reasonable consumer acting reasonably under the circumstances.

87. These misrepresentations have resulted in consumer injury or harm to the public interest.

88. As a result of these misrepresentations, Plaintiff and members of the Class have suffered economic injury including, but not limited to, violations of their rights of privacy and loss of value in their personally identifiable information.

89. On behalf of herself and other Subclass members, Plaintiff seeks to enjoin the unlawful acts and practices described herein, to recover her actual damages or five hundred dollars, whichever is greater, reasonable attorneys' fees and costs, and any other just and proper relief available under Section 350 of the New York General Business Law.

WHEREFORE, Plaintiff prays for relief and judgment, as follows:

- a. Determining that this action is a proper class action;

- b. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure, naming Plaintiff as representative of the Class and Subclass and naming Plaintiff's attorneys as Class Counsel to represent the Class and Subclass;
- c. For an order declaring that Defendant's conduct violates the statutes referenced herein;
- d. For an order finding in favor of Plaintiff and the Class and Subclass on all counts asserted herein;
- e. Award compensatory damages, including statutory damages where available, to Plaintiff and the Class and Subclass members against Defendant for all damages sustained as a result of Defendant's wrongdoing, in an amount to be proven at trial;
- f. Ordering Defendant to disgorge revenues and profits wrongfully obtained;
- g. For prejudgment interest on all amounts awarded;
- h. For injunctive relief ordering Defendant to immediately cease its illegal conduct;
- i. For an order awarding Plaintiff and the Class their reasonable attorneys' fees and expenses and costs of suit; and
- j. Grant Plaintiff and the Class members such further relief as the Court deems appropriate.

JURY DEMAND

Plaintiff hereby demands a trial by jury on all claims so triable in this action.

Dated: February 4, 2025

Respectfully submitted,

By: /s/ Alec Leslie

BURSOR & FISHER, P.A.

Alec M. Leslie

1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Tel: (646) 837-7150
Fax: (212) 989-9163
E-Mail: aleslie@bursor.com

BURSOR & FISHER, P.A.
Stephen A. Beck (*pro hac vice* forthcoming)
701 Brickell Ave., Suite 2100
Miami, FL 33131
Tel: (305) 330-5512
Fax: (305) 676-9006
E-Mail: sbeck@bursor.com

Attorneys for Plaintiff