IN THE UNITED STATES DISTRICT COURT
FOR THE NOTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

A.G., individually and on behalf of all others similarly situated, Plaintiff, v. THERAPYMATCH, INC. d/b/a HEADWAY, Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff A.G. ("Plaintiff") brings this class action complaint on behalf of herself and all others similarly situated (the "Class Members") against Defendant Therapymatch, Inc. d/b/a Headway ("Defendant" or "Headway"). Plaintiff brings this action based on personal knowledge of the facts pertaining to herself, and on information and belief as to all other matters, by and through the investigation of undersigned counsel.

NATURE OF THE ACTION

1. Plaintiff brings this suit on behalf of all LinkedIn users who live in the United States and who scheduled a therapy appointment through the website www.headway.co (the "Website").

2. When individuals seek therapy, they often share sensitive personal information, including mental health history, personal struggles, and other confidential medical information. Data privacy is especially vital when booking therapy online, primarily due to the sensitive nature of this protected medical information. When patients engage in online therapy, they must be able to trust that their information is protected from unauthorized disclosure to third parties. When patients know their information is secure, they are more likely to pursue the support they

need without fear of judgment or exposure. This is particularly important in therapy, where societal stigma around mental health can already be a barrier to accessing care.

3. Information related to therapy appointments is protected by state and federal law, including the Health Insurance Portability and Accountability Act ("HIPAA"). Therapy providers are legally required to safeguard patients' health information. This means that any data related to a patient's mental health, treatment history, and personal circumstances surrounding the reason for booking an appointment must be kept confidential and secure. Given these protections, patients reasonably expect that information related to their therapy appointments will remain confidential.

4. However, unbeknownst to Plaintiff and members of the putative class, Defendant aided, employed, agreed, and conspired with LinkedIn to intercept these sensitive and confidential communications, including information concerning the medical conditions for which they were seeking therapy. Defendant failed to receive consent for these interceptions.

5. LinkedIn develops, owns, and operates "the world's largest professional network with more than 1 billion members in more than 200 countries and territories worldwide."[1] LinkedIn is also an advertising company, that touts its ability to deliver targeted marketing to specific users.

6. Plaintiff brings this action on behalf of herself and the Class (as defined below) for equitable relief and to recover damages and restitution for: (i) violation of the Electronic Communications Privacy Act ("ECPA") 18 U.S.C. § 2511(1), *et seq.*; and (ii) negligence.

PARTIES

7. Plaintiff is an Illinois citizen who resides in Chicago, Illinois. At all relevant

[1] LINKEDIN, ABOUT, https://about.linkedin.com/?trk=homepage-basic_directory_aboutUrl.

times, Plaintiff maintained an active LinkedIn account.

8. Plaintiff scheduled several therapy appointments through the Website from approximately April through June, 2024. When searching for a therapist on the Website, Plaintiff disclosed that she was looking for mental health treatment related to "relationship issues," "identity issues," "eating disorders," "trauma," and "stress." Pursuant to the systemic process described herein, Defendant assisted LinkedIn with intercepting Plaintiff's communications, including those that contained personally identifiable information ("PII") and protected health information ("PHI"). This includes information related to the medical reasons for the appointment and the specific therapist she was seeing. Defendant assisted LinkedIn's interceptions without Plaintiff's knowledge, consent, or express written authorization.

9. By failing to receive the requisite consent, Defendant breached its duty of confidentiality and aided LinkedIn in unlawfully intercepting Plaintiff's PII and PHI. Such acts are an egregious violation of Plaintiff's right to privacy.

10. Defendant Therapymatch, Inc. is a Delaware corporation with a principal place of business in New York, New York. Defendant owns and operates the website www.headway.co. Defendant's Website is an online healthcare platform that matches patients with therapists for therapy appointments for various mental health conditions. Defendant embedded a software code known as the LinkedIn Insight Tag on its Website, as described in more detail below. Defendant embedded this tracking technology on its Website for advertising purposes.

JURISIDICTION AND VENUE

11. This Court has subject matter jurisdiction under 28 U.S.C. § 1331 over the claims that arise under the Electronic Communications Privacy Act, 18 U.S.C. § 2510, *et seq* ("ECPA").

12. This Court also has subject matter 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 interest and costs.

13. This Court has personal jurisdiction over Defendant because Defendant conducts substantial business in this District.

14. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to the claim occurred within this District.

FACTUAL ALLEGATIONS

A. Mental Health Information is Sensitive and Confidential

15. Defendant assisted LinkedIn with intercepting information that is sensitive, confidential, and personally identifiable.

16. Defendant is a healthcare company that hosts a website to connect patients with therapists for mental health treatment.

17. Under federal law, a healthcare provider may not disclose PII or PHI without the patient's express written authorization.[2]

18. 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."[3]

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

[3] U.S. Dept. of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.

19. 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 of causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual."[4]

20. 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.*

21. 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.

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

a. Failing to ensure the confidentiality and integrity of electronic PHI that Headway 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.R.F. 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 Headway 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

[4] 42 U.S.C. § 1320d-6.

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).

23. Health care organizations regulated under HIPAA, like Defendant, may use third-party tracking tools, such as the LinkedIn Insight Tag, *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 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**.[5]

24. 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,

[5] 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.

> 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.**[6]

25. 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.

26. 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**.[7]

27. 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.[8]

28. 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:

---

[6] *Id.* (emphasis added).

[7] *Id.* (emphasis added).

[8] *Id.* (emphasis added).

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 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.[9]

29. Therefore, Defendant's conduct, as described more thoroughly below, is directly

[9] 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.

contrary to federal law and the clear pronouncements by the FTC and HHS.

B. LinkedIn's Platform and Business Tools

30. LinkedIn markets itself as "the world's largest professional network on the internet[.]"[10] But LinkedIn is no longer simply a tool to help users find jobs or expand their professional network. LinkedIn has moved into the marketing and advertising space, and boasts of its ability to allow potential advertisers to "[r]each 1 billion+ professionals around the world" via its Marketing Solutions services.[11] Recently, LinkedIn was projected as being responsible for "roughly 0.9 percent of the global ad revenue" which included approximately $5.91 billion in advertising revenue in 2022.[12]

31. According to LinkedIn, "[t]argeting is a foundational element of running a successful advertising campaign — [g]etting your targeting right leads to higher engagement, and ultimately, higher conversion rates."[13] Targeting refers to ensuring that advertisements are targeted to, and appear in front of, the target demographic for an advertisement. To that end, LinkedIn's Marketing Solutions services allow potential advertisers to "[b]uild strategic campaigns" targeting specific users.[14] LinkedIn's "marketing solutions allow advertisers to select specific characteristics to help them reach their ideal audience. The ads [users] see on

---

[10] LINKEDIN, WHAT IS LINKEDIN AND HOW CAN I USE IT?, https://www.linkedin.com/help/linkedin/answer/a548441#.

[11] LINKEDIN, MARKETING SOLUTIONS, https://business.linkedin.com/marketing-solutions.

[12] Valentina Dencheva, *LinkedIn annual ad revenue 2017-2027*, STATISTA (Dec. 12, 2023), https://www.statista.com/statistics/275933/linkedins-advertising-revenue.

[13] LINKEDIN, REACH YOUR AUDIENCE: TARGETING ON LINKEDIN, p.3, https://business.linkedin.com/content/dam/me/business/en-us/marketing-solutions/resources/pdfs/linkedin-targeting-playbook-v3.pdf.

[14] LinkedIn, *supra* note 11.

LinkedIn are then targeted to provide content relevant to [the users]."[15]

32. As a result of its activities and operation of the LinkedIn Insight Tag, LinkedIn is able to make extremely personal inferences about individuals' demographics, intent, behavior, engagement, interests, buying decisions, and more.[16]

33. The personal information and communications obtained by LinkedIn are used to fuel various services offered via LinkedIn's Marketing Solutions including Ad Targeting, Matched Audiences, Audience Expansion, and LinkedIn Audience Network.[17]

34. Such information is extremely valuable to marketers and advertisers because the inferences derived from users' personal information and communications allows marketers and advertisers, including healthcare providers and insurance companies, to target potential customers.[18]

35. For example, through the use of LinkedIn's Audience Network, marketers and

---

[15] LINKEDIN, LINKEDIN ADS AND MARKETING SOLUTIONS, https://www.linkedin.com/help/lms/answer/a421454.

[16] *See* LINKEDIN, MARKETING SOLUTIONS, https://business.linkedin.com/marketing-solutions/audience ("Target audiences through demographic marketing[,]" "Zero in on intent, behavior, engagement, interests, and more[,]" and "Reach the LinkedIn audience involved in the buying decision").

[17] *See id.*

[18] LINKEDIN, PRIVACY POLICY, https://www.linkedin.com/legal/privacy-policy ("We serve you tailored ads both on and off our Services. We offer you choices regarding personalized ads, but you cannot opt-out of seeing other ads."); LINKEDIN, ACCOUNT TARGETING, https://business.linkedin.com/marketing-solutions/ad-targeting ("Target your ideal customer based on traits like their job title, company name or industry, and by professional or personal interests"); LINKEDIN, EXAMPLES OF TRENDING AND BEST-IN-CLASS HEALTHCARE CAMPAIGNS AND CONTENT, p.6, https://business.linkedin.com/content/dam/me/business/en-us/marketing-solutions/healthcare-microsite/resources/lkin-lms-sales-healthcare-campaigns-trending-content-Jan2023.pdf ("BD zeroed in on the end-benefit with a 30 second video introducing their PIVO needle-free blood collection device to potential customers."); LINKEDIN, HEALTHCARE SOCIAL MEDIA STRATEGIES FOR 2023, p.1, https://business.linkedin.com/content/dam/me/business/en-us/marketing-solutions/healthcare-microsite/resources/hc-social-media-trends.pdf (listing "potential customers" as "Common audiences" for insurance sector).

advertisers are able to expand their reach and advertise on sites other than LinkedIn to "reach millions of professionals across multiple touchpoints."[19] According to Broc Munro of Microsoft, "[w]e gravitate towards social platforms like LinkedIn to achieve more targeted marketing engagement. However, we know that our audiences don't spend all their time on social media. LinkedIn Audience Network enables us to expand our reach to trusted sites while still respecting our audience targeting. This increases the impact of our advertising."[20]

36. In July 2022, "LinkedIn Marketing Solutions surpassed $5 billion in annual revenue[.]"[21] That figure is "expected to further grow to reach 10.35 billion U.S. dollars by 2027."[22]

37. According to LinkedIn, the LinkedIn Insight Tag is "[a] simple code snippet added to [a] website [that] can help you optimize your campaigns, retarget your website visitors, and learn more about your audiences."[23] LinkedIn represents that the LinkedIn Insight Tag "enable[s] in-depth campaign reporting and unlock[s] valuable insights about your website visitors."[24]

38. LinkedIn's current iteration of its Insight Tag is a JavaScript-based code which

---

[19] LinkedIn, Account Targeting, https://business.linkedin.com/marketing-solutions/ad-targeting.

[20] LINKEDIN, LINKEDIN AUDIENCE NETWORK, https://business.linkedin.com/marketing-solutions/native-advertising/linkedin-audience-network.

[21] *LinkedIn Business Highlights from Microsoft's FY22 Q4 Earnings*, LINKEDIN PRESSROOM (July 25, 2022), https://news.linkedin.com/2022/july/linkedin-business-highlights-from-microsoft-s-fy22-q4earnings#:~:text=And%20LinkedIn%20Marketing%20Solutions%20surpassed,revenue%20for%20the%20first%20time.

[22] Dencheva, *supra* note 12.

[23] LINKEDIN, INSIGHT TAG, https://business.linkedin.com/marketing-solutions/insight-tag.

[24] LINKEDIN, LINKEDIN INSIGHT TAG FAQS, https://www.linkedin.com/help/lms/answer/a427660.

allows for the installation of its software.[25] A critical feature allows the LinkedIn Insight Tag to track users, even when third-party cookies are blocked.[26] LinkedIn "recommend[s] using the JavaScript-based Insight Tag or Conversions API" because third-party cookie settings are being deprecated across the industry.[27] Embedding the JavaScript as a first-party cookie causes users' browsers to treat the LinkedIn Insight Tag as though it is offered by the website being visited, rather than by LinkedIn. Doing so ensures that the third-party cookie-blocking functions of modern web browsers do not prevent LinkedIn from collecting data through its software.[28] Instead, the LinkedIn Insight Tag is shielded with the same privacy exemptions offered to first-party cookies.

39. When a user who has signed in to LinkedIn (even if the user subsequently logs out) is browsing a website where the LinkedIn Insight Tag has been embedded, an HTTP request is sent using cookies, which includes information about the user's actions on the website.

40. These cookies also include data that differentiate users from one another and can be used to link the data collected to the user's LinkedIn profile.

41. The HTTP request about an individual who has previously signed into LinkedIn includes requests from the "li_sugr" and "lms_ads" cookies. Each of these cookies are used by LinkedIn "to identify LinkedIn Members off LinkedIn" for advertising purposes.[29]

42. For example, the "li_sugr" cookie is "[u]sed to make a probabilistic match of a

---

[25] LINKEDIN, *supra* note 23.

[26] *Id.* ("It's important for advertisers to prepare for these changes by switching to JavaScript tags and enabling 'enhanced conversion tracking' in the Insight Tag settings to continue capturing signals where 3rd party cookies are blocked.").

[27] *See id.*

[28] *See id.*

[29] LINKEDIN, LINKEDIN COOKIE TABLE, https://www.linkedin.com/legal/l/cookie-table.

user's identity."[30] Similarly, the "lms_ads" cookie is "[u]sed to identify LinkedIn Members off LinkedIn for advertising."[31]

43. A LinkedIn profile contains information including an individual's first and last name, place of work, contact information, and other personal details. Based on information it obtains through the LinkedIn Insight Tag, Defendant LinkedIn is able to target its account holders for advertising.

44. LinkedIn never receives consent from users to intercept and collect electronic communications containing their sensitive and unlawfully-disclosed information. In fact, LinkedIn expressly warrants the opposite.

45. When first signing up, a user agrees to the User Agreement.[32] By using or continuing to use LinkedIn's Services, users agree to two additional agreements: the Privacy Policy[33] and the Cookie Policy.[34] For California residents, LinkedIn also publishes a California Privacy Disclosure.[35]

46. LinkedIn's Privacy Policy begins by stating that "LinkedIn's mission is to connect the world's professionals . . . . Central to this mission is our commitment to be transparent about the data we collect about you, how it is used and with whom it is shared."[36]

47. The Privacy Policy goes on to describe what data LinkedIn collects from various

---

[30] *See id.*

[31] *See id.*

[32] LINKEDIN, USER AGREEMENT, https://www.linkedin.com/legal/user-agreement.

[33] LINKEDIN, PRIVACY POLICY, https://www.linkedin.com/legal/privacy-policy.

[34] LINKEDIN, COOKIE POLICY, https://www.linkedin.com/legal/cookie-policy.

[35] LINKEDIN, CALIFORNIA PRIVACY DISCLOSURE, https://www.linkedin.com/legal/california-privacy-disclosure.

[36] LINKEDIN, PRIVACY POLICY, *supra* note 33.

sources, including cookies and similar technologies. LinkedIn states "we use cookies and similar technologies (e.g., pixels and ad tags) to collect data (e.g., device IDs) to recognize you and your device(s) on, off and across different services and devices where you have engaged with our Services. We also allow some others to use cookies as described in our Cookie Policy."[37]

48. However, LinkedIn offers an express representation: "**We will only collect and process personal data about you where we have lawful bases**."[38]

49. Despite this explicit representation, LinkedIn intentionally intercepts and receives sensitive and unlawfully disclosed information in violation of state and federal privacy laws.

50. Users never choose to provide sensitive information to LinkedIn because, among other reasons, they never know whether a particular website uses the LinkedIn Insight Tag, and, if so, what sensitive personal data it collects.

C. Defendant Assisted LinkedIn With Intercepting It's Patients PII and PHI

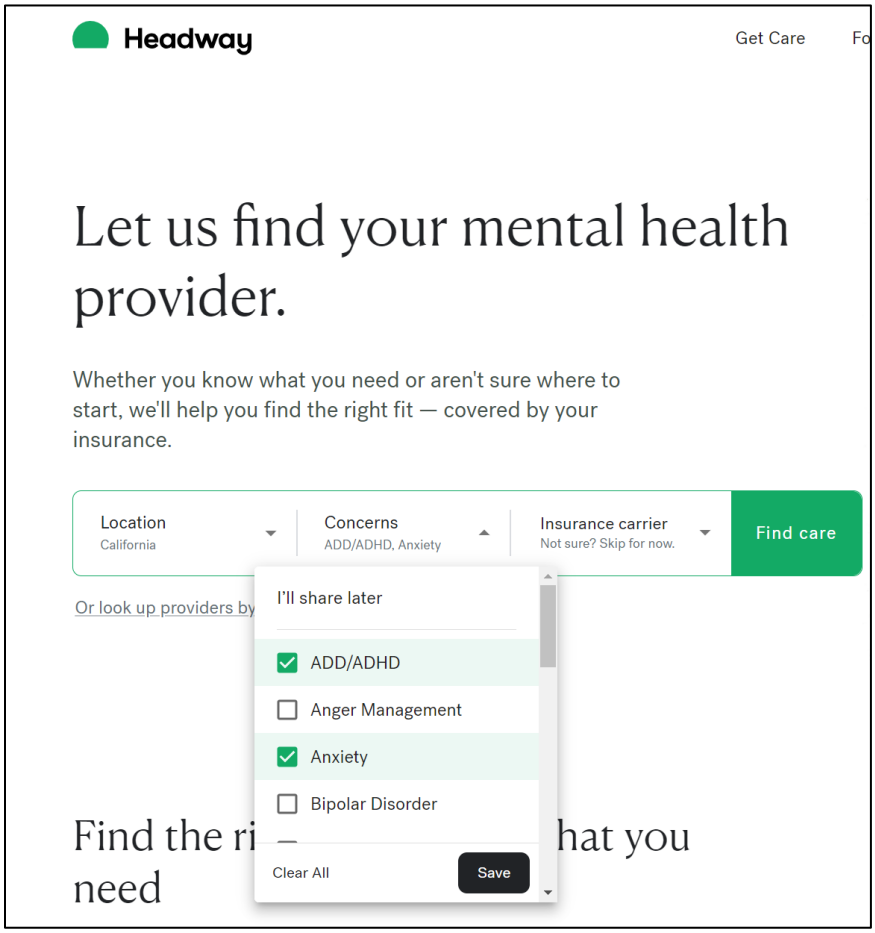
51. Headway is an online healthcare operator that connects patients with therapists. Upon entering the Website, Headway warrants that it will help "find your mental health provider."

52. To begin, patients must provide Headway with certain information to find available therapists that will fit their mental health needs, including their location, concerns, and insurance carrier.

[37] *See id.*

[38] *See id.* (emphasis added).

Figure 1:



53. Unbeknownst to consumers, LinkedIn was tracking their activity the moment they entered the Headway Website.

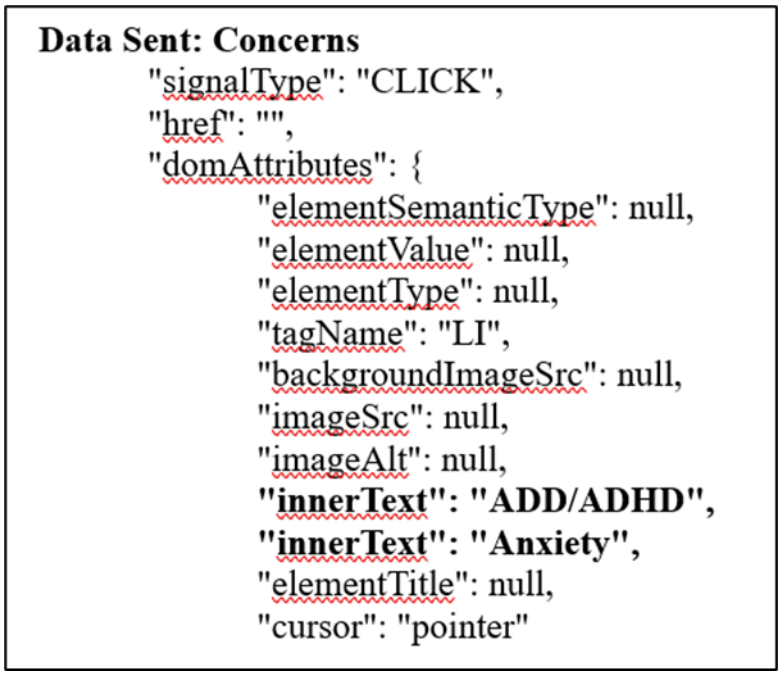
54. For example, the LinkedIn Insight Tag was embedded on the Website, which allowed LinkedIn to intercept and record "click" events. Click events detail information about which page on the Website the patient was viewing as well as the selections they were making.

55. Through the LinkedIn Insight Tag, Defendant aided LinkedIn in intercepting consumers confidential information related to their therapy appointments in order to monetize that data for targeted advertising.

56. For example, when a patient provides their information, as shown above in Figure

1, and clicks "Find care," LinkedIn intercepts their confidential information through the LinkedIn Insight Tag.

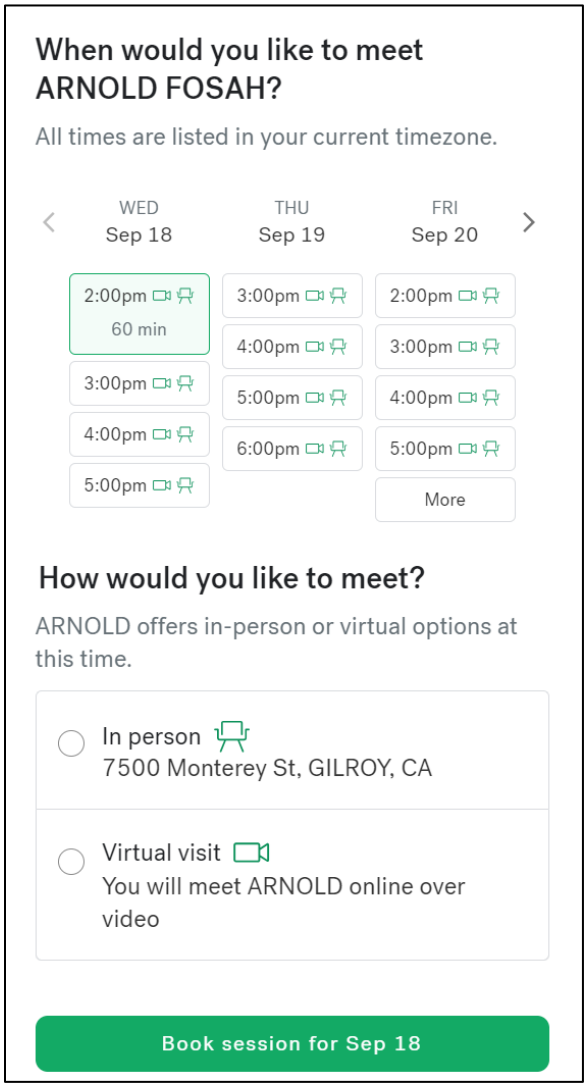
Figure 2:



57. Patients then continue through Defendant's Website to select their preferred therapist.

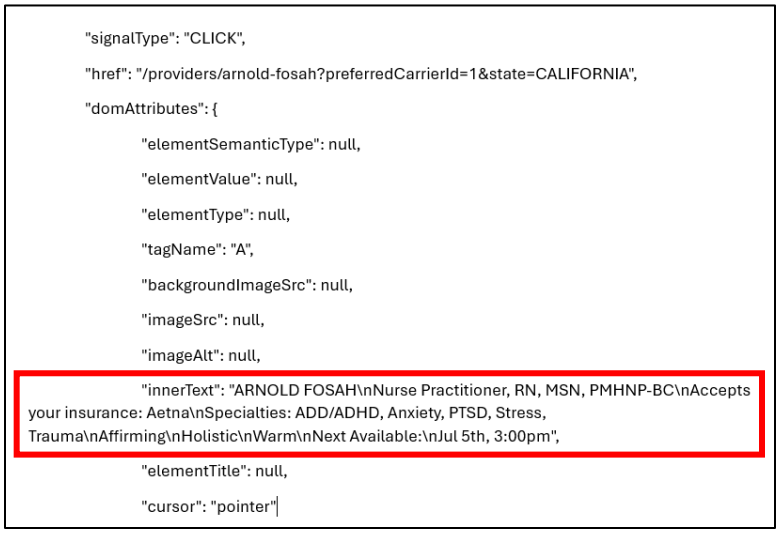
58. After providing additional details and confirming an appointment with their preferred therapist, Defendant aids Linkedn in intercepting that information through the LinkedIn Insight Tag as well.

Figure 3:



59. As shown in Figure 4 below, LinkedIn intercepts several pieces of confidential information, including the name of the patient's therapist, the medical reasons for the therapy appointment, and the date and time of the appointment.

Figure 4:



60. These interceptions also included the li_sugr and lms_ads cookies, which LinkedIn utilizes to identify its account holders for targeted advertising.

61. LinkedIn incorporated the information it intercepted from the Headway Website into its marketing tools to fuel its targeted advertising service.

62. Plaintiff never consented, agreed, authorized, or otherwise permitted LinkedIn to intercept her confidential health information.

63. By law, Plaintiff is entitled to privacy in her protected health information and confidential communications. Defendant deprived Plaintiff of her privacy rights when it implemented a system that surreptitiously tracked and recorded Plaintiff's and other online consumers' confidential communications, personally identifiable information, and protected health information.

CLASS ACTION ALLEGATIONS

64. Plaintiff seeks to represent a class defined as all LinkedIn account holders in the United States, excluding California, who booked a therapy appointment on www.headway.co (the "Class").

65. Subject to additional information obtained through further investigation and discovery, the foregoing definition of the Class may be expanded or narrowed by amendment to the complaint or narrowed at class certification.

66. The "Class Period" is the time period beginning on the date established by the Court's determination of any applicable statute of limitations, after consideration of any tolling, concealment, and accrual issues, and ending on the date of entry of judgement.

67. Specifically excluded from the Class are Defendant, Defendant's officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, employees, principals, servants, partners, joint ventures, or entities controlled by Defendant, and their heirs, successors, assigns, or other persons or entities related to or affiliated with Defendant and/or Defendant's officers and/or directors, the judge assigned to this action, and any member of the judge's immediate family.

68. **Numerosity.** The members of the proposed Class are geographically dispersed throughout the United States and are so numerous that individual joinder is impracticable. Upon information and belief, Plaintiff reasonably estimates that there are thousands of individuals that are members of the proposed Class. Although the precise number of proposed members are unknown to Plaintiff, the true number of members of the Class are known by Defendant. Members of the Class may be notified of the pendency of this action by mail and/or publication through the records of Defendant and third-party LinkedIn.

69. **Typicality.** The claims of the representative Plaintiff are typical of the claims of the Class in that the representative Plaintiff, like all members of the Class, scheduled a therapy appointment on the Website and had her confidential information disclosed to a third party. The representative Plaintiff, like all members of the Class, has been damaged by Defendant's

misconduct in the very same way as the members of the Class through the privacy violations alleged herein. Further, the factual bases of Defendant's misconduct are common to all members of the Class and represent a common thread of misconduct resulting in injury to all members of the Class.

70. **Existence and predominance of common questions of law and fact.** Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting only individual members of the Class. These common legal and factual questions include, but are not limited to, the following:

a. Whether Defendant intentionally tapped the lines of internet communication between patients and their healthcare provider;

b. Whether Defendant's Website surreptitiously recorded personally identifiable information, protected health information, and related communications and subsequently, or simultaneously, disclosed that information to LinkedIn;

c. Whether LinkedIn is a third-party eavesdroppers;

d. Whether Defendant's disclosures of personally identifiable information, protected health information, and related communications constituted an affirmative act of communication;

e. Whether Defendant's conduct, which allowed LinkedIn—an unauthorized person—to view Plaintiff's and Class Members' personally identifiable information and protected health information, resulted in a breach of confidentiality;

f. Whether Defendant violated Plaintiff's and Class Members' privacy rights by using the LinkedIn Insight Tag to record and communicate patients' confidential

medical communications; and

g. Whether Defendant breached its duty owed to Plaintiff and the Class by disclosing their PII and PHI to LinkedIn.

71. **Adequacy of Representation.** Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff has retained counsel who are highly experienced in complex consumer class action litigation, and Plaintiff intends to vigorously prosecute this action on behalf of the Class. Plaintiff has no interests that are antagonistic to those of the Class.

72. **Superiority.** A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by members of the Class are relatively small compared to the burden and expense of individual litigation of her claims against Defendant. It would, thus, be virtually impossible for members of the Class, on an individual basis, to obtain effective redress for the wrongs committed against them. Furthermore, even if members of the Class could afford such individualized litigation, the court system could not. Individualized litigation would create the danger of inconsistent or contradictory judgments arising from the same set of facts. Individualized litigation would also increase the delay and expense to all parties and the court system from the issues raised by this action. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, economies of scale, and comprehensive supervision by a single court, and presents no unusual management difficulties under the circumstances.

73. In the alternative, the Class may be certified because:

(a) the prosecution of separate actions by individual members of the Class would create a risk of inconsistent or varying adjudication with respect to individual members of the Class that would establish incompatible standards of conduct for the Defendant;

(b) the prosecution of separate actions by individual members of the

Class would create a risk of adjudications with respect to them that would, as a practical matter, be dispositive of the interests of other members of the Class not parties to the adjudications, or substantially impair or impede her ability to protect her interests; and/or

(c) Defendant has acted or refused to act on grounds generally applicable to the Class as a whole, thereby making appropriate final declaratory and/or injunctive relief with respect to the members of the Class as a whole.

CAUSES OF ACTION

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

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

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

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

77. 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.

78. 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).

79. 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).

80. 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).

81. 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).

82. 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).

83. The following instruments constitute "devices" within the meaning of the ECPA:

a. The computer codes and programs LinkedIn 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 LinkedIn's web and ad servers;

e. The plan Defendant and LinkedIn 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.

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

85. By utilizing and embedding the LinkedIn Insight Tag 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).

86. Specifically, Defendant intercepted Plaintiff's and Class Members' electronic communications through the LinkedIn Insight Tag, which tracked, stored and unlawfully disclosed Plaintiff's and Class Members' PII and PHI to third parties, such as LinkedIn.

87. Defendant intercepted communications that include, but are not necessarily limited to, communications to/from Plaintiff and Class Members regarding PII and PHI, including their treatment information. This confidential information was then matched to patients' LinkedIn accounts and monetized for targeted advertising purposes.

88. 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).

89. 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).

90. 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.

91. 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.[39]

92. Plaintiff's information that Defendant disclosed to LinkedIn 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 wire or electronic communications to increase its profit margins. Defendant specifically used the LinkedIn Insight Tag to track and utilize Plaintiff's and Class Members' PII and PHI for financial gain.

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

94. 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 through the LinkedIn Insight Tag. Plaintiff and Class Members, all of whom are patients of Defendant, had a reasonable expectation that Defendant would not redirect their communications to

[39] 42 U.S.C. § 1320d-6.

LinkedIn without their knowledge or consent.

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

96. 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
Negligence

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

98. Defendant knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' PII and PHI, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, misused, and disclosed to unauthorized parties.

99. As a provider of health care under the law, Defendant had a special relationship with Plaintiff and Class Members who entrusted Defendant to adequately protect their PII and PHI.

100. Defendant knew that the PII and PHI at issue was private and confidential and should be protected as private and confidential. Thus, Defendant owed a duty of care not to subject Plaintiff and Class Members to an unreasonable risk of unauthorized disclosure.

101. Defendant knew, or should have known, of the risks inherent in collecting and storing PII and PHI and allowing it to be accessed by unauthorized third parties.

102. Defendant's failure to take proper security measures to protect Plaintiff's and Class Members' PII and PHI created conditions conducive to a foreseeable risk of unauthorized access

and disclosure of such confidential information to unauthorized third parties. As described above, Plaintiff and Class Members are part of a foreseeable, discernable group that was at high risk of having their confidential information compromised, and otherwise wrongly disclosed if not adequately protected by Defendant.

103. Defendant had a duty under common law to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' PII and PHI.

104. Defendant owed a duty to timely and adequately inform Plaintiff and Class Members, in the event of their PII and PHI being improperly disclosed to unauthorized third parties.

105. Defendant systematically failed to provide adequate security for data in its possession or over which it had supervision and control.

106. Defendant, through its actions and omissions, unlawfully breached duties to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' PII and PHI within Defendant's possession, supervision, and control.

107. Defendant, through its actions and omissions, unlawfully breached duties owed to Plaintiff and Class Members by failing to have appropriate procedures in place to prevent dissemination of Plaintiff's and Class Members' PII and PHI.

108. Defendant, through its actions and omissions, unlawfully breached duties to timely and fully disclose to Plaintiff and Class Members that the PII and PHI within Defendant's possession, supervision, and control was improperly accessed by unauthorized third parties, the nature of this access, and precisely the type of information improperly accessed.

109. Defendant's breach of duties owed to Plaintiff and Class Members proximately

caused Plaintiff's and Class Members' PII and PHI to be compromised by being accessed by unauthorized third parties.

110. As a result of Defendant's ongoing failure to adequately notify Plaintiff and Class Members regarding what type of PII and PHI has been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages.

111. As a proximate result of Defendant's negligence and breach of duties as set forth above, Defendant's breaches of duty caused Plaintiff and Class Members to, inter alia, have their data shared with third parties without their authorization or consent, receive unwanted advertisements that reveal seeking treatment for specific medical conditions, fear, anxiety and worry about the status of their PII and PHI, diminution in the value of their personal data for which there is a tangible value, and/or a loss of control over their PII and PHI, all of which can constitute actionable actual damages.

112. In failing to secure Plaintiff's and Class Members' PII and PHI, Defendant is guilty of oppression, fraud, or malice. Defendant acted or failed to act with a reckless, willful, or conscious disregard of Plaintiff's and Class Members' rights. Plaintiff, in addition to seeking actual damages, also seeks punitive damages on behalf of herself and the Class.

113. Defendant's conduct in violation of applicable laws directly and proximately caused the unauthorized access and disclosure of Plaintiff's and Class Members' PII and PHI, and as a result, Plaintiff and Class Members have suffered and will continue to suffer damages as a result of Defendant's conduct. Plaintiff and Class Members seek actual, compensatory, and punitive damages, and all other relief they may be entitled to as a proximate result of Defendant's negligence.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests, individually and on behalf of the alleged Class, that the Court enter judgment in her favor and against Defendant as follows:

(a) For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure, naming Plaintiff as the representative for the Class, and naming Plaintiff's attorneys as Class Counsel to represent the Class;

(b) For an order declaring that Defendant's conduct violates the causes of action referenced herein;

(c) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

(d) For compensatory, statutory, and punitive damages in amounts to be determined by the Court and/or jury;

(e) For prejudgment interest on all amounts awarded;

(f) For an order of restitution and all other forms of equitable monetary relief;

(g) For injunctive relief as pleaded or as the Court may deem proper; and

(h) For an order awarding Plaintiff and the Class their reasonable attorneys' fees and expenses and costs of suit.

DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of any and all issues in this action so triable as of right.

Dated: September 23, 2024

Respectfully Submitted,

By: */s/ Alec M. Leslie*
Alec M. 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.
Sarah N. Westcot (*pro hac vice* forthcoming)
Stephen A. Beck
701 Brickell Avenue, Suite 2100
Miami, FL 33131
Telephone: (305) 330-5512
Facsimile: (305) 676-9006
E-Mail: swestcot@bursor.com
sbeck@bursor.com

Attorneys for Plaintiff