Exhibit A1

IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

RONDA COOPER, CORAL FRASER, DAVID GITLIN and GILBERT MANDA, *on behalf of themselves and all others similarly situated*, Plaintiffs, v. MOUNT SINAI HEALTH SYSTEM, INC., Defendant.	Case No. 23-9485 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Ronda Cooper, Coral Fraser, David Gitlin and Gilbert Manda, through their attorneys, bring this class action lawsuit in their individual capacities and on behalf of all others similarly situated against Mount Sinai Health System, Inc. ("Mount Sinai" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents or other related entities. Plaintiffs allege the following on information and good faith belief—except as to their own actions, their counsel's investigations and facts of public record.

INTRODUCTION

1. This case concerns a very serious breach of Mount Sinai's data privacy and security obligations as it installed certain tracking technologies on its digital properties to collect and disclose to unauthorized third parties Plaintiffs' and Class Members' personally identifiable information ("PII") and protected health information ("PHI") (collectively referred to as "PII/PHI" or "Private Information") for its own pecuniary gain.

2. Information concerning a person's physical and mental health is among the most confidential and sensitive information in our society, and the mishandling of such information can have serious consequences, including, but certainly not limited to, discrimination in the workplace and/or denial of insurance coverage.[1]

3. Simply put, if people do not trust that their sensitive private medical information will be kept private and secure, they may be less likely to seek medical treatment, which can lead to more serious health consequences down the road. In addition, protecting medical information and making sure it is kept confidential and not disclosed to anyone other than the person's medical providers is vital to maintaining public trust in the healthcare system as a whole.

4. Reiterating the importance of and necessity for data security and privacy concerning health information, the Federal Trade Commission ("FTC") recently published a bulletin entitled *Protecting the privacy of health information: A Baker's dozen takeaways from FTC cases*, in which it noted that "[h]ealth information is not just about medications, procedures, and diagnoses. ***Rather, it is anything that conveys information—or enables an inference—about a consumer's health***. Indeed, [recent FTC enforcement actions involving] *Premom*, *BetterHelp*, *GoodRx* and *Flo Health* ***make clear that the fact that a consumer is using a particular health-related app or website—one related to mental health or***

[1] *See* Lindsey Ellefson, *Telehealth Sites Put Addiction Patient Data at Risk: New research found pervasive use of tracking tech on substance-abuse-focused health care websites, potentially endangering users in a post-Roe world*, WIRED (Nov. 16, 2022), *available at* https://www.wired.com/story/substance-abuse-telehealth-privacy-tracking-tech/ (last visited Oct. 24, 2023) ("While the sharing of any kind of patient information is often strictly regulated or outright forbidden, it's even more verboten in addiction treatment, as patients' medical history can be inherently criminal and stigmatized.").

fertility, for example—or how they interact with that app (say, turning 'pregnancy mode' on or off) may itself be health information."[2]

5. The FTC is unequivocal in its stance as it informs—in no uncertain terms—healthcare companies that they should ***not*** use tracking technologies to collect sensitive health information and disclose it to various platforms without informed consent:

> ***Don't use behind-the-scenes tracking technologies that contradict your privacy promises or otherwise harm consumers.***
>
> In today's surveillance economy, the consumer is often the product. Consumer data powers the advertising machine that goes right back to the consumer. ***But when companies use consumers' sensitive health data for marketing and advertising purposes, such as by sending that data to marketing firms via tracking pixels on websites or software development kits on apps, watch out.***
>
> [Recent FTC enforcement actions such as] *BetterHelp*, *GoodRx*, *Premom*, and *Flo* make clear that practices like that ***may run afoul of the FTC Act if they violate privacy promises or if the company fails to get consumers' affirmative express consent for the disclosure of sensitive health information***.[3]

6. Defendant Mount Sinai systematically violates its patients' medical privacy rights, exposing their highly sensitive personal information to third parties without their knowledge or

[2] *See* Elisa Jillison, *Protecting the privacy of health information: A Baker's dozen takeaways from FTC cases*, the FTC Business Blog (July 25, 2023) (emphasis added), *available at* https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases (last visited Oct. 25, 2023).

[3] *Id.* (emphasis added) (further noting that *GoodRx* & *Premom* underscore that this conduct may also violate the Health Breach Notification Rule, which requires notification to consumers, the FTC and, in some cases, the media, of disclosures of health information without consumers' authorization.

consent. In particular, Mount Sinai impermissibly discloses its patients' Private Information without their consent.

7. Mount Sinai owns and controls a website, https://www.mountsinai.org/ (the "Website"), which it encourages patients to use to book medical appointments, locate physicians and treatment facilities, communicate medical symptoms, search medical conditions and treatment options, sign up for events and classes and much more.

8. Mount Sinai also controls and maintains a web-based patient portal (the "Portal") whereby registered users can access their MyChart to, among other things, communicate with their healthcare providers, access lab and test results, manage prescriptions and request refills, as well as make and manage medical appointments.[4]

9. The MyChart patient portal is a software system designed and licensed to Mount Sinai by Epic Software Systems ("Epic"). Epic is a privately owned healthcare software company that provides services to 250 million patients, including two-thirds of the United States population.

10. Epic's MyChart software system was designed to permit licensees—such as Mount Sinai—to deploy "custom analytics scripts" within MyChart, including, for example, the Facebook Pixel or Google Analytics, which all for the transmission of PII, including medical and health-related information and communications to third parties.[5]

11. The Website and the Portal are referred to herein as the "Web Properties."

[4] *See* https://mychart.msmc.com/MyChart/Authentication/Login? (last visited Oct. 24, 2023).

[5] *See* Todd Feathers, Simon Fondrie-Teitler, Angie Waller & Surya Mattu, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, THE MARKUP (June 16, 2022), *available at* https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites (last visited Oct. 24, 2023).

12. Plaintiffs and Class Members who visited and used Defendant's Web Properties (collectively, the "Users") understandably thought they were communicating only with their trusted healthcare providers. Unbeknownst to Plaintiffs and Class Members; however, Defendant had embedded an undetectable tracking Pixel on its Web Properties, which automatically transmits to Meta Platforms, Inc., d/b/a Meta ("Facebook") every click, keystroke and intimate detail about their medical symptoms, conditions and treatments (the "Pixel" or "Facebook Pixel").

13. As a result, hospitals that use analytics tools like the Facebook Pixel or Google Analytics on their websites may also have those tools embedded on the MyChart login page or even inside the MyChart patient portal.

14. Operating as designed and as implemented by Mount Sinai, the Pixel allows the Private Information that Plaintiffs and Class Members provide to Defendant in furtherance of their health treatment to be unlawfully disclosed to Facebook alongside the individual's unique and persistent Facebook ID ("FID").[6]

15. A pixel is a piece of code that "tracks the people and [the] type of actions they take"[7] as they interact with a website, including how long a person spends on a particular web page, which buttons the person clicks, which pages they view and the text or phrases they type into various portions of the website (such as a general search bar, chat feature or text box).

[6] The Pixel forces the website user to share the FID for easy tracking via the "cookie" Facebook stores every time someone accesses their Facebook account from the same web browser. "Cookies are small files of information that a web server generates and sends to a web browser"; "[c]ookies help inform websites about the user, enabling the websites to personalize the user experience." *See* https://www.cloudflare.com/learning/privacy/what-are-cookies/ (last visited Oct. 24, 2023).

[7] RETARGETING, https://www.facebook.com/business/goals/retargeting (last visited Oct. 24, 2023).

16. The user's web browser (software applications that allow consumers to exchange electronic communications over the Internet) executes the Pixel via instructions within the webpage to communicate certain information based on parameters selected by the website's owner. The Facebook Pixel is thus customizable and programmable, meaning that the website owner controls which of its web pages contain the Pixel and which events are tracked and transmitted to Facebook.

17. By installing the Facebook Pixel, Defendant effectively planted a bug on Plaintiffs' and Class Members' web browsers and compelled them to unknowingly disclose their private, sensitive and confidential health-related communications with Defendant to Facebook.

18. In addition to the Facebook Pixel, Defendant, upon information and good faith belief, also installed and implemented Facebook's Conversions Application Programming Interface ("CAPI") on its Web Properties servers.[8]

19. Unlike the Facebook Pixel, which co-opts a website user's browser and forces it to disclose information to third parties in addition to the website owner, CAPI does not cause the User's browser to transmit information directly to Facebook. Rather, CAPI tracks the User's website interaction, including Private Information, records and stores that information on the website owner's servers and then transmits the data to Facebook from the website owner's servers.[9]

[8] CAPI "works with your Facebook pixel to help improve the performance and measurement of your Facebook ad campaigns." *See* https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/ (last visited Oct. 24, 2023).

[9] "Server events are linked to a dataset ID and are processed like events sent via the Meta Pixel…. This means that server events may be used in measurement, reporting, or optimization in a similar way as other connection channels," https://revealbot.com/blog/facebook-conversions-api/ (last visited Oct. 24, 2023).

20. Indeed, Facebook markets CAPI as a "better measure [of] ad performance and attribution across your customer's full journey, from discovery to conversion. This helps you better understand how digital advertising impacts both online and offline results."[10]

21. Despite the clear and unequivocal prohibition on the disclosure of PHI without consent, Mount Sinai chose to use the Pixel and CAPI data for marketing purposes in an effort to bolster its profits. That is, despite professing to "provide compassionate patient care with seamless coordination and to advance medicine through unrivaled education, research, and outreach in the many diverse communities we serve,"[11] Defendant put its desire for profit over its patients' privacy rights.

22. The Facebook Pixel and CAPI are routinely used to target specific customers by utilizing data to build incredibly fulsome and robust profiles for the purposes of retargeting and future marketing. Facebook also uses Plaintiffs' and Class Members' Private Information to create targeted advertisements based on the medical conditions and other Private Information disclosed to Defendant.

23. The information that Defendant's Tracking Pixel and CAPI sent to Facebook included the Private Information that Plaintiffs and Class Members submitted to Defendant's Website, including, for example, patient status, medical treatment sought, diagnosed health condition and the fact that the individual attempted to or did book a medical appointment.

[10] *See* https://www.facebook.com/business/help/2041148702652965?id=818859032317965 (last visited Oct. 24, 2023).

[11] https://www.mountsinai.org/about/mission (last visited Oct. 24, 2023).

24. Such information allows a third party (e.g., Facebook) to know that a specific patient was seeking confidential medical care. Facebook, in turn, sells Plaintiffs' and Class Members' Private Information to third-party marketers who geo-target Plaintiffs' and Class Members' Facebook pages based on communications obtained via the Facebook Pixel and CAPI.[12]

25. Healthcare patients simply do not anticipate that their trusted healthcare provider will send Private Information collected via its web pages to an undisclosed third party—let alone Facebook, which has a sordid history of privacy violations in pursuit of ever-increasing advertising revenue—without the patients' informed and express consent.

26. Neither Plaintiffs nor any other Class Members were provided, much less signed, a written authorization permitting Defendant to disclose their Private Information to Facebook.

27. Despite willfully and intentionally incorporating the Facebook Pixel and CAPI into its Website and servers, Defendant has never disclosed to Plaintiffs or Class Members that it shared their sensitive and confidential communications and Private Information with Facebook,[13] the

[12] Facebook and any third-party purchasers of Plaintiffs' and Class Members' Private Information also could reasonably infer from the data that a specific patient was being treated for a specific type of medical condition, such as cancer, pregnancy, dementia or HIV.

[13] In contrast to Defendant, in recent months, several medical providers that had installed the Facebook Pixel on their web properties have provided their patients with notices of data breaches caused by the Pixel transmitting PHI to third parties. *See, e.g.*, *Cerebral, Inc. Notice of HIPAA Privacy Breach*, *available at* https://cerebral.com/static/hippa_privacy_breach-4000c6eb21449c2ecd8bd13706750cc2.pdf (last visited Oct. 24, 2023); *Advocate Aurora says 3M patients' health data possibly exposed through tracking technologies* (Oct. 20, 2022), *available at* https://www.fiercehealthcare.com/health-tech/advocate-aurora-health-data-breach-revealed-pixels-protected-health-information-3 (last visited Oct. 24, 2023); *Novant Health notifies patients of potential data privacy incident* (Aug. 12, 2022), *available at* https://www.novanthealth.org/home/about-us/newsroom/press-releases/newsid33987/2672/novant-health-notifies-patients-of-potential-data-privacy-incident-.aspx (last visited Oct. 24, 2023).

largest social media company on earth, which has a sordid history of privacy violations in pursuit of ever-increasing advertising revenue.[14]

28. Plaintiffs and Class Members were unaware that their Private Information was being surreptitiously transmitted to Facebook as they communicated with their healthcare providers via the Web Properties or that their information was stored on Defendant's servers to be later transmitted to Facebook so it could be used for targeted advertising and marketing purposes.

29. The disclosure of Plaintiffs' and Class Members' Private Information via the Pixel contravenes the letter and spirit of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). As part of HIPAA, the United States Department of Health and Human Services ("HHS") established "Standards for Privacy of Individually Identifiable Health Information" (also known as the "Privacy Rule"), which governs how healthcare providers must safeguard and protect Private Information.

30. Simply put, covered entities such as Defendant are ***not*** permitted to use tracking technology tools (like pixels) in a way that exposes patients' Private Information to any third-party without express and informed consent from each patient.

31. Lest there be any doubt of the illegal nature of Defendant's practice, the Office for Civil Rights (OCR) at HHS has made clear, in a recent bulletin entitled *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, that the unlawful transmission of such protected information violates HIPAA's Privacy Rule:

[14] This Court will not have to look far to find evidence of Meta's violations of privacy laws. Just in May of this year the European Union fined Meta "a record-breaking" $1.3 billion for violating EU privacy laws. *See* Hanna Ziady, *Meta slapped with record $1.3 billion EU fine over data privacy*, https://www.cnn.com/2023/05/22/tech/meta-facebook-data-privacy-eu-fine/index.html (last accessed Oct. 25, 2023).

> 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.***[15]

32. As recently as February 2023 (and potentially through April 2023), Mount Sinai routinely disclosed its patients' PII/PHI—such as their status as patients, their providers, their medical care and treatment options, search queries, appointments, the hospitals they visited and their personal identities—to Facebook. And, as of the date of the filing of this complaint, Mount Sinai continues to disclose such information to Google and other third parties. Mount Sinai did this without its patients' knowledge, authorization, or consent.

33. Mount Sinai breached its obligations in one or more of the following ways: (i) failing to adequately review its marketing programs and web-based technology to ensure the Web Properties was safe and secure; (ii) failing to remove or disengage technology that was known and designed to share web users' information; (iii) failing to obtain the consent of Plaintiffs and Class Members to disclose their PII and PHI to Facebook or others; (iv) failing to take steps to block the transmission of Plaintiffs' and Class Members' PII and PHI through the Facebook Pixel; (v) failing to warn Plaintiffs and Class Members; and (vi) otherwise failing to design and monitor its Web Properties to maintain the confidentiality and integrity of patient PII and PHI.

34. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct; these injuries include: (i) invasion of privacy, (ii) loss of benefit of the bargain,

[15] *See Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates, available at* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited Oct. 24, 2023) (emphasis added).

(iii) compromise and disclosure of Private Information and identities, (iv) diminution of value of their Private Information, (iv) statutory damages and (v) the continued and ongoing risk to their Private Information.[16]

35. Plaintiffs seek to remedy these harms and therefore assert causes of action for (i) Invasion of Privacy, (ii) Breach of Contract; (iii) Breach of Fiduciary Duty; (iv) Unjust Enrichment; (v) Breach of Implied Contract; (vi) Breach of Confidence; (vii) Bailment; (viii) Violation of New York's Deceptive Trade Practices Act (New York Gen. Bus. Law § 349); (ix)-(x) Violations of the Wiretap Act (18 U.S.C. § 2510, *et seq.*); (xi) Violation of the Stored Communications Act (18 U.S.C. § 2702, *et seq.*); and (xii) Violation of the Computer Fraud and Abuse Act (18 U.S.C. § 1030, *et seq.*).

PARTIES

36. Plaintiff Ronda Cooper is a natural person residing in Queens County in the State of New York, where he intends to remain.

37. Plaintiff Coral Fraser is a natural person residing in New York County in the State of New York, where she intends to remain.

38. Plaintiff David Gitlin is a natural person residing in New York County in the State of New York, where he intends to remain.

39. Plaintiff Gilbert Manda is a natural person residing in New York County in the State of New York, where he intends to remain.

[16] The exposed Private Information of Plaintiffs and Class Members can—and likely will—be further disseminated to additional third parties utilizing the data for retargeting or insurance companies utilizing the information to set insurance rates. Furthermore, third parties can often offer for sale the unencrypted, unredacted Private Information to criminals on the dark web for use in fraud and cyber-crimes.

40. As detailed herein, Plaintiffs accessed Mount Sinai's Web Properties on their computers and mobile devices and used the Web Properties to look for providers, review conditions and treatments, make appointments and communicate with their providers. Plaintiffs have used and continue to use the same devices to maintain and access active Facebook accounts throughout the relevant period in this case.

41. Further to the systematic process described herein, Defendant assisted Facebook with intercepting Plaintiffs' communications, including those that contained PII, PHI and related confidential information. Defendant assisted in these interceptions without Plaintiffs' knowledge, consent or express written authorization.

42. Defendant Mount Sinai is a registered non-profit entity with its headquarters, principal place of business and main campus at One Gustave L. Levy Place, New York, NY 10029.

43. Defendant Mount Sinai is one of the oldest and largest teaching hospitals in the United States, with eight hospital campuses and thirteen free-standing joint venture centers.[17]

44. Defendant is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d and 45 C.F.R. Part 160-45 C.F.R. Part 162 and 45 C.F.R. Part 164 ("HIPAA").

JURISDICTION & VENUE

45. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1331 because it arises under the laws of the United States and under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000,

[17] *See* https://www.mountsinai.org/about/facts (last visited Oct. 24, 2023).

exclusive of interest and costs, there are more than 100 members in the proposed class and at least one member of the class is a citizen of a state different from Defendant.

46. This Court has personal jurisdiction over Defendant because its principal place of business is in this District, and a substantial portion of the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this District.

47. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District.

COMMON FACTUAL ALLEGATIONS

A. Defendant Improperly Disclosed Plaintiffs' & Class Members' Private Information.

48. Defendant's clinical enterprise consists of eight hospital campuses—Mount Sinai Beth Israel, Mount Sinai Brooklyn, The Mount Sinai Hospital, Mount Sinai Queens, Mount Sinai Morningside, Mount Sinai West (formerly Mount Sinai Roosevelt), New York Eye and Ear Infirmary of Mount Sinai and Mount Sinai South Nassau. Defendant's also have thirteen free-standing joint venture centers—six endoscopy centers, five ambulatory surgery centers and two urgent care joint ventures.[18]

49. As the owner and operator of these medical centers and entities, Defendant offers a wide range of services, from primary and urgent care to cancer treatment, cardiology, geriatrics, orthopedics and orthopedic surgery and neurology.[19]

50. Defendant utilized Facebook advertisements and intentionally installed the Pixel and CAPI on its Web Properties.

---

[18] *See id.*

[19] *See* https://www.mountsinai.org/find-a-doctor/specialties (last visited Oct. 25, 2023).

51. The Pixel is a piece of code that Defendant commonly used to measure activity and experiences on its Web Properties.

52. CAPI is another tool that Defendant used to track its users' actions on its Web Properties, including by avoiding ad blockers that can prevent the Pixel from gathering users' data.

53. Through seeking and using Defendant's services as a medical provider and utilizing the Web Properties services, Plaintiffs' and Class Members' Private Information was intercepted in real-time and then disseminated to Facebook, and potentially to other third parties, via the Pixel that Defendant surreptitiously installed on its Web Properties.

54. Plaintiffs and Class Members did not intend or had any reason to suspect their Private Information would be shared with Facebook or that Defendant was tracking their every movement and disclosing it to Facebook when they provided highly sensitive information on the Web Properties.

55. Defendant did not disclose to or warn Plaintiffs or Class Members that Defendant used the Private Information contained in Plaintiffs' and Class Members' Web Properties submissions for marketing purposes.

56. Plaintiffs and Class Members never consented, agreed, authorized or otherwise permitted Defendant to disclose their Private Information.

57. Upon information and belief, Defendant intercepted and disclosed the following non-public private information to Facebook:

a. Plaintiffs' and Class Members' status as medical patients;

b. Plaintiffs' and Class Members' communications with Defendant through its Web Properties, including specific text queries typed into the search bar, medical conditions for which they sought treatments

and treatments sought;

c. Plaintiffs' and Class Members' searches for appointments, appointment details, location of treatments, medical providers and their specialties, medical conditions and treatments;

d. PII, including but not limited to patients' locations, IP addresses, device identifiers and an individual's unique Facebook ID.

58. Defendant deprived Plaintiffs and Class Members of their privacy rights when it: (i) implemented technology (*i.e.*, Pixels) that surreptitiously tracked, recorded and disclosed Plaintiffs' and other online patients' confidential communications and Private Information; (ii) disclosed patients' protected information to Facebook—an unauthorized third-party; and (iii) undertook this pattern of conduct without notifying Plaintiffs or Class Members and without obtaining their express written consent.

B. Background on Facebook's Platform & its Business Tools.

59. Facebook operates the world's largest social media company and generated $117 billion in revenue in 2021.[20] Roughly 97% of that came from selling advertising space.[21]

60. As a core part of its business, Facebook maintains profiles on users that include the user's real names, locations, email addresses, friends, likes and communications that Facebook associates with personal identifiers, such as IP addresses.

[20] FACEBOOK, META REPORTS FOURTH QUARTER AND FULL YEAR 2021 RESULTS, https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx (last visited Oct. 25, 2023).

[21] *Id.*

61. Facebook also tracks non-Facebook users through its widespread internet marketing products and source code.[22]

62. Facebook encourages and promotes entities and website owners, such as Defendant, to utilize its "Business Tools" to gather, identify, target and market products and services to individuals.

63. The Business Tools are automatically configured to capture certain data, like when a user visits a webpage, that webpage's Universal Resource Locator ("URL") and metadata, or when a user downloads a mobile application or makes a purchase.[23]

64. Facebook's Business Tools can also track other events. Facebook offers a menu of "standard events" from which advertisers can choose, including what content a visitor views or purchases.[24] Advertisers can even create their own tracking parameters by building a "custom event."[25]

---

[22] Source code may also command a web browser to send data transmissions to third parties via pixels or web bugs, tiny 1x1 invisible GIF files that effectively open a spying window through which a website funnels data about users and their actions to third parties.

[23] *See* FACEBOOK PIXEL, ACCURATE EVENT TRACKING, ADVANCED, https://developers.facebook.com/docs/facebook-pixel/advanced/; *see also* BEST PRACTICES FOR FACEBOOK PIXEL SETUP, https://www.facebook.com/business/help/218844828315224?id=1205376682832142 (last visited Oct. 24, 2023); APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited Oct. 24, 2023).

[24] SPECIFICATIONS FOR FACEBOOK PIXEL STANDARD EVENTS, https://www.facebook.com/business/help/402791146561655?id=1205376682832142 (last visited Oct. 24, 2023).

[25] ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, https://www.facebook.com/business/help/964258670337005?id=1205376682832142 (last visited Oct. 24, 2023); *see also* FACEBOOK, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited Oct. 24, 2023).

65. One Business Tool is the Facebook Pixel. Facebook offers this code to advertisers, like Defendant, to integrate into their websites. As the name implies, the Facebook Pixel "tracks the people and type of actions they take."[26]

66. When a user accesses a website hosting the Facebook Pixel, Facebook's software script surreptitiously directs the user's browser to send a separate message to Facebook's servers. This second, secret transmission contains the original GET request sent to the host website, along with additional data that the Facebook Pixel is configured to collect.

67. This transmission is initiated by Facebook code and concurrent with the communications with the host website. Two sets of code are thus automatically run as part of the browser's attempt to load and read Defendant's Web Properties—Defendant's own code and Facebook's embedded code.

68. Facebook causes the browser to secretly duplicate the communication with Defendant, transmitting it to Facebook's servers, alongside additional information that transcribes the communication's content and the individual's identity. Consequently, when Plaintiffs and Class Members visited Defendant's Web Properties and entered sensitive search terms (e.g., Breast or Prostate Cancer, Diabetes Management or AIDS Treatment) on Defendant's Web Properties, their Private Information was transmitted to Facebook, including, but not limited to, physician and appointment selected, treatments and care options and specific button/menu selections.

69. Plaintiffs' and Class Members' identities could be easily determined based on the FID, IP address and/or reverse lookup from the collection of other identifying information that was improperly disclosed.

[26] RETARGETING, *supra* note 7.

70. Notably, this transmission ***only*** occurs on webpages that contain the Pixel. Thus, Plaintiffs' and Class Member's Private Information would ***not*** have been disclosed to Facebook via the Pixel but for Defendant's decision to install the Pixel on its Web Properties. Plaintiffs' and Class Member's Private Information would not have been disclosed to Facebook via CAPI but for Defendant's decision to install and use that tool.

71. Similarly, Plaintiffs' and Class Members' Private Information would not have been disclosed to Facebook via CAPI but for Defendant's decision to install and implement that tool.

72. By installing and implementing both tools, Defendant caused Plaintiffs' and Class Members communications to be intercepted and transmitted to Facebook via the Pixel, and it caused a second improper disclosure of that information via CAPI.

C. How Mount Sinai Discloses Class Members' Protected Health Information and Assists with Intercepting Communications

73. When patients visit Defendant's Web Properties via an HTTP Request to Mount Sinai's server, Defendant's server sends an HTTP Response, including the Markup that displays the Webpage visible to the user and Source Code (with the Pixel).[27]

74. The patient visiting this web page only sees the Markup, ***not*** Defendant's Source Code or underlying HTTP Requests and Responses.

75. Defendant's Source Code manipulates the patient's browser by secretly instructing it to duplicate the patient's communications (HTTP Requests) and to send those communications

[27] An HTTP request is an electronic communication sent from the client device's browser to the website's server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (*i.e.*, web address), GET Requests can also send data to the host server embedded inside the URL, and can include cookies. An HTTP response is an electronic communication that is sent as a reply to the client device's web browser from the host server in response to an HTTP Request. HTTP Responses may consist of a web page, another kind of file, text information, or error codes, among other data.

to Facebook, including full string URLs containing terms entered into search fields and fillable forms, button click data and keystrokes.

76. This occurs because the Pixel embedded in Mount Sinai's Source Code is programmed to automatically track and transmit Users' communications contemporaneously, invisibly and without patient knowledge.

77. Thus, without consent, Defendant has effectively used its source code to commandeer patients 'computing devices, thereby re-directing their Private Information to third parties.

78. Tracking codes embedded on Defendant's Web Properties, including Pixel and CAPI, sent non-public Private Information to Facebook, including but not limited to Plaintiffs' and Class Members': (1) status as medical patients; (2) health conditions; (3) sought treatment or therapies; (4) appointment requests and appointment booking information; (5) registration or enrollment in medical classes (such as breastfeeding courses); (6) locations or facilities where treatment is sought; (7) which webpages were viewed and (8) phrases and search queries conducted via the general search bar.

79. Third parties, like Facebook, place third-party cookies in the web browsers of users logged into their platforms. These cookies uniquely identify the user and are sent with each intercepted communication to ensure the third-party can identify the patient associated with the Personal Information intercepted.

80. With substantial work and technical know-how, internet users can sometimes circumvent this browser-based wiretap technology; that is why third parties bent on gathering Private Information, like Facebook, implement workarounds that savvy users cannot evade.

81. Facebook's workaround, for example, is called CAPI, which is an effective workaround because it does not intercept data communicated from the user's browser. Instead, CAPI "is designed to create a direct connection between [Web hosts'] marketing data and [Facebook]."

82. Thus, the private communications between Users and Mount Sinai, which are necessary to use its Web Properties, are actually received by Defendant and stored on its server before CAPI collects and sends the Private Information contained in those communications directly from Defendant to Facebook.

83. Client devices do not have access to host servers and thus cannot prevent (or even detect) this transmission.

84. Importantly, the Private Information Defendant's Pixel sent to Facebook was sent alongside the Plaintiffs' and Class Members' Facebook ID (c_user cookie or FID), thereby allowing individual patients 'communications with Defendant and the Private Information contained in those communications to be linked to their unique Facebook accounts.[28]

85. A user's FID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the user, including pictures, personal interests, work history, relationship status and other details. Because the user's FID uniquely identifies an individual's Facebook account, Meta—or any ordinary person—can easily use the FID to quickly and easily locate, access and view the user's corresponding Facebook profile. To find the Facebook

[28] Defendant's Web Properties track and transmit data via first-party and third-party cookies. The c_user cookie or FID is a type of third-party cookie assigned to each person who has a Facebook account, and it is comprised by a unique and persistent set of numbers.

account associated with a c_user cookie, one simply needs to type www.facebook.com/ followed by the c_user ID.

D. Defendant's Pixel Disseminates Patient Information via its Web Properties

86. Defendant deprived Plaintiffs and Class Members of their privacy rights when it: (1) implemented technology (i.e., the Facebook Pixel) that surreptitiously tracked, recorded and disclosed Plaintiffs' and other online patients 'confidential communications and Private Information; (2) disclosed patients 'protected information to Facebook—an unauthorized third-party; and (3) undertook this pattern of conduct without notifying Plaintiff or Class Members and without obtaining their express written consent.

87. For example, when a patient visits https://www.mountsinai.org/ to search for a doctor, they may select the "Find a Doctor" tab, which takes them to the "Find a Doctor" page.

88. Upon information and good faith belief, Defendant's webpages for its various hospitals operate the same way as Defendant's general Website, and share their patients' identities and online activity, including information and search results related to their private medical conditions and treatment.

89. If a patient selects filters or enters keywords into the search bar on the "Find a Doctor" webpage, the filters and search terms, including the doctor's specialty, are transmitted via the Facebook Pixel.

90. Similarly, if a patient uses the Website's general search bar, the terms and phrases the patient types are transmitted to Facebook, even if they contain a patient's treatment, procedures, medical conditions or related queries. This information is automatically sent from the patient's device to Facebook, revealing the patient's FID (c_user field) along with each search filter the patient selected.

91. After taking any of these actions on the "Find a Doctor" page, patients are subsequently directed to the page with "search results," and their selections or search parameters are automatically transmitted to Facebook. The information transmitted to Facebook includes: (i) the patient's unique and persistent FID (c_user ID), (ii) the fact that the patient clicked on a specific provider's profile page, (iii) the patient's search parameters (demonstrating they specifically searched for a doctor's specialty) and (iv) the patient's location.

92. Defendantinstalled at least two Pixels on its Web Properties, including a Pixel with ID number "940133619402530" which identified and categorized which actions the User took on the webpage at issue (including "PageView" which identifies the User as having viewed the particular webpage, "Microdata" which contains page metadata, and "SubscribedButtonClick," which tracks each click on the webpage and shares the metadata of buttons clicked by the User, such the "inner text" of the button, with Facebook). Defendant also installed a Pixel with ID number "194331831908198" which also collected "PageView" events.

93. Defendant's Website also includes a feature that allows patients to book appointments through a particular doctor's profile page. If a patient clicks on the "Request Appointment" button, this action is communicated and shared with Facebook, including, upon information and good faith belief, the provider's name and/or specialty.

94. If a patient finishes the process of making an appointment, this action is also communicated and shared with Facebook.

95. Similarly, each doctor's profile page includes a direct link that allows a patient to call the doctor's office, and upon clicking the telephone number button, the patient's click is shared with Facebook.

96. Each time Defendant sends this activity data, it discloses a patient's PII and PHI.

97. Finally, Defendant also notifies Facebook of its patients' patient status. For example, when a user accesses Defendant's page to utilize Defendant's patient portal, Defendant notifies Facebook of that as well.

98. Mount Sinai's Website also provides a link to MyMountSinai (MyChart) on each page of its Website. When a patient clicks on this link, that information (i.e., that the patient is accessing MyChart, and thus, presumptively, a patient of Mount Sinai), is sent to Facebook.

99. Defendant has re-configured the Pixels on many of its webpages. As a result, Plaintiffs are unable to determine whether the Pixels were embedded inside the MyChart portal. However, given Defendant's use of the Pixels on other pages of the Website (including the "book appointment" page, which tells Facebook that a patient booked an appointment with a specific doctor, and the log-in page for the MyChart portal), Plaintiffs reasonably believe and, therefore, aver that Defendant used the Pixels to track information on its entire digital platform, including inside its MyChart portal.

100. A user who accesses Defendant's Web Properties while logged (or having recently logged) into Facebook will transmit the c_user cookie to Facebook, which contains that user's unencrypted FID.

101. When accessing the Website, for example, Facebook receives at least seven cookies[29]:

[29] Not pictured here is the _fbp cookie, which is transmitted as a first-party cookie.

Name	Value	Domain	P...	Expires / Max-Age	S...
presence	C%7B%22t3%...	.facebook.com	/	Session	75
sb	GrxtY1jj9lKWn...	.facebook.com	/	2024-04-06T23:4...	26
datr	QtI1Y1lVd2UW...	.facebook.com	/	2024-04-05T23:1...	28
xs	7%3A_7bqKp6...	.facebook.com	/	2024-10-23T20:4...	99
wd	1664x993	.facebook.com	/	2023-10-31T20:4...	10
fr	1BhquGXZpTh...	.facebook.com	/	2024-01-22T20:4...	84
c_user	54(	.facebook.com	/	2024-10-23T20:4...	15

Figure 1

102. When a visitor's browser has recently logged out of an account, Facebook compels the visitor's browser to send a smaller set of cookies.

103. The fr cookie contains, at least, an encrypted FID and browser identifier.[30] Facebook, at a minimum, uses the fr cookie to identify users.[31]

104. At each stage, Defendant also utilized the _fbp cookie, which attaches to a browser as a first-party cookie, and Facebook uses to identify a browser and a user:[32]

Name	Value	Domain	P...	Expires / Max-Age
_fbp	fb.1.1696430267150.1195488401	.mountsinai.org	/	2024-01-24T15:15...

Figure 2. The fbp_ cookie value being shared with Facebook.

105. The fr cookie expires after 90 days unless the visitor's browser logs back into Facebook.[33] If that happens, the time resets, and another 90 days begins to accrue.

---

[30] Data Protection Commissioner, *Facebook Ireland Ltd: Report of Re-Audit* (Sept. 21, 2012), p. 33, http://www.europe-v-facebook.org/ODPC_Review.pdf (last visited Oct. 24, 2023).

[31] COOKIES & OTHER STORAGE TECHNOLOGIES, https://www.facebook.com/policy/cookies/ (last visited Oct. 24, 2023).

[32] *Id.*

[33] *Id.*

106. The _fbp cookie expires after 90 days unless the visitor's browser accesses the same website.[34] If that happens, the time resets and another 90 days begins to accrue.

107. The Facebook Tracking Pixel uses both first- and third-party cookies. A first-party cookie is "created by the website the user is visiting"—i.e., Defendant.[35] A third-party cookie is "created by a website with a domain name other than the one the user is currently visiting"—i.e., Facebook.[36]

108. The _fbp cookie is always transmitted as a first-party cookie. A duplicate _fbp cookie is sometimes sent as a third-party cookie, depending on whether the browser has recently logged into Facebook.

109. Facebook, at a minimum, uses the fr, _fbp, and c_user cookies to link to FIDs and corresponding Facebook profiles.

110. As described *infra*, Defendant sent these identifiers with the event data.

111. Plaintiffs never consented, agreed, authorized, or otherwise permitted Defendant to disclose their PII/PHI; nor did they authorize any assistance with intercepting their communications. Plaintiffs were never provided with any written notice that Defendant disclosed its Web Properties' users' PHI, nor were they provided any means of opting out of such disclosures. Despite this, Defendant knowingly disclosed Plaintiffs' PHI to Facebook.

---

[34] *Id*.

[35] *First-Party Cookie*, https://www.pcmag.com/encyclopedia/term/first-party-cookie (last visited Oct. 24, 2023). This is confirmable by using developer tools to inspect a website's cookies and track network activity *Id*.

[36] *Third-Party Cookie*, https://www.pcmag.com/encyclopedia/term/third-party-cookie (last visited Oct. 24, 2023). This is also confirmable by tracking network activity.

112. By law, Plaintiffs are entitled to privacy in their PHI and confidential communications. Defendant deprived Plaintiffs and Class Members of their privacy rights when it: (i) implemented a system that surreptitiously tracked, recorded and disclosed Plaintiffs' and Class Members' confidential communications, PII and PHI to a third party; (ii) disclosed patients' protected information to Facebook—an unauthorized third-party eavesdropper; and (iii) undertook this pattern of conduct without notifying Plaintiffs and Class Members and without obtaining their express written consent. Plaintiffs did not discover that Defendant disclosed their PII and PHI to Facebook, and assisted Facebook with intercepting their communications, until at least February 8, 2023 for Plaintiffs Cooper, Fraser, Gitlin and Manda.

E. Defendant's Privacy Policies & Promises.

113. Defendant publishes several privacy policies that represent to patients and visitors to its Website that Mount Sinai will keep Private Information private and secure and that it will only disclose PII and PHI provided to it under certain circumstances, ***none of which apply here***.

114. Defendant publishes Mount Sinai Privacy Policy, which tells patients: "MOUNT SINAI employs a variety of online security measures to safeguard and keep your information private."[37]

115. Defendant's Privacy Policy further states, "MOUNT SINAI ***does not*** share your personally identifiable information with third parties without your consent, except for third-party suppliers that perform essential business or administrative services for us (for example, our web hosting provider). MOUNT SINAI provides these suppliers only with the information they need

[37] https://www.mountsinai.org/privacy#:~:text=MOUNT%20SINAI%20reserves%20the%20right,ii)%20to%20release%20information%20in (last visited Oct. 25, 2023).

to perform such services and asks that they either comply with this Privacy Policy or maintain comparable privacy policies that protect your personally identifiable information."[38]

116. Defendant's Notice of Privacy Practices explains Defendant's legal duties with respect to Private Information and the exceptions for when Defendant can lawfully use and disclose Plaintiffs' and Class Members' Private Information in the following ways:

- Treatment;
- Payment;
- Business operations;
- Appointment reminders, treatment alternatives, benefits and services;
- Fundraising ("We will not sell your PHI without your authorization.");
- Business associates ("we will have a written contract with them that requires the BA and any of its subcontractors to protect the privacy of your PHI. They and their subcontractors are independently required by federal law to protect your information.");
- In-Patient Directory;
- Family and friends involved in your care;
- As required by law;
- Public health activities;
- Victims of abuse, neglect or domestic violence;
- Health oversight activities,
- Product monitoring, repair and recall;
- Lawsuits and disputes;
- Law enforcement;
- To avert a serious and imminent threat to health or safety;
- National security and intelligence activities or protective services;
- Military and veterans;
- Inmates and correctional institutions;
- Workers' compensation;
- Coroners, medical examiners and funeral directors;
- Organ and tissue donation;
- Research;
- Completely de-identified of partially de-identified information;
- Incidental disclosures ("While we will take reasonable steps to safeguard the privacy of your PHI, certain disclosures of your PHI may occur during or as an unavoidable result of our otherwise permissible uses or disclosures

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

of your PHI"). [39]

117. Defendant's Privacy Policy does ***not*** permit Defendant to use nor disclose Plaintiffs' and Class Members' PHI for marketing purposes.

118. Mount Sinai also acknowledges that it is "required by law to protect the privacy of your health information."[40]

119. Mount Sinai breached their own privacy policies by unlawfully intercepting and disclosing Users' Private Information to Facebook (and likely other third parties) without obtaining patients' consent or authorization.

F. Defendant Violated HIPAA.

120. Defendant's disclosure of Plaintiffs' and Class Members' Private Information to entities like Facebook also violated HIPAA.

121. Under federal law, a healthcare provider may not disclose PII, non-public medical information about a patient, potential patient, or household member of a patient for marketing purposes without the patient's express written authorization.[41]

122. Guidance from the United States Department of Health and Human Services instructs healthcare providers that patient status alone is protected by HIPAA.

123. In Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, the Department instructs:

---

[39] https://www.mountsinai.org/files/MSHealth/Assets/HS/About/Compliance/Notice-of-Privacy-Practices-NOPP%20-English.pdf (last visited Oct. 25, 2023).

[40] *Id*.

[41] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data… If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.[42]

124. In its guidance for Marketing, the Department further instructs:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, *covered entities may not sell lists of patients to third* parties without obtaining authorization from each person on the list. (Emphasis added).[43]

125. Under HIPAA, an IP address is considered PII:

a. HIPAA defines PII to include "any unique identifying number, characteristic or code" and specifically lists the example of IP addresses. *See* 45 C.F.R. § 164.514 (2).

b. HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information." 45 C.F.R. § 164.514(2)(ii); *See* also, 45 C.F.R. § 164.514(b)(2)(i)(O).

126. Facebook, Google and other third-party marketing companies track IP addresses to track and target individual homes and their occupants with advertising.

---

[42] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (last visited Oct. 24, 2023).

[43] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf (last visited Oct. 24, 2023).

127. Consequently, Defendant's disclosure of patients' IP addresses violated HIPAA and industry privacy standards.

128. Defendant's placing of third-party tracking code on its Web Properties is a violation of Plaintiffs' Class Members' privacy rights under federal law.[44]

G. Defendant Violated Industry Standards.

129. A medical provider's duty of confidentiality is embedded in the physician-patient and hospital-patient relationship—it is a cardinal rule.

130. The American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications.

131. AMA Code of Ethics Opinion 3.1.1 provides:

> Protecting information gathered in association with the care of the patient is a core value in health care… Patient privacy encompasses a number of aspects, including, … personal data (informational privacy)[.][45]

132. AMA Code of Medical Ethics Opinion 3.2.4 provides:

> Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (a) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's

[44] While Plaintiffs do not bring a claim under HIPAA itself, this violation evidences Defendant's wrongdoing as relevant to other claims.

[45] https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/code-of-medical-ethics-chapter-3.pdf (last visited Oct. 24, 2023).

> authorized surrogate when the individual lacks decision-making capacity about the purposes for which access would be granted.[46]

133. AMA Code of Medical Ethics Opinion 3.3.2 provides:

> Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically…must: (c) Release patient information only in keeping with ethics guidelines for confidentiality.[47]

H. Defendant Violated New York Standards.

134. New York State has long been a national leader in protecting the confidentiality of personal medical information and has strict privacy standards for medical records.

135. Unlike HIPAA, New York requires patient consent before a physician can disclose an individual's medical information to another treating physician and limits disclosure to immediately relevant information.[48]

[46] *Id*.

[47] *Id*.

[48] *See* New York Public Health Law § 18(6).

136. Even stronger protections restrict the release of certain especially sensitive information regarding genetic tests,[49] mental health,[50] medical treatment of adolescents,[51] sexually transmitted infections[52] and HIV.[53]

137. New York State Department of Health regulations governing hospitals impose significant privacy and security standards relating to medical records, patient rights and medical staff by-laws.

138. With respect to medical records, a hospital must ensure the confidentiality of patient records and release records or information from records "only to hospital staff involved in treating the patient and individuals as permitted by Federal and State laws."[54]

139. This provision has been interpreted to require hospitals to obtain consent from the patient prior to disclosing medical records to an outside entity, even for treatment or reimbursement purposes.[55]

140. A hospital must also institute safeguards to protect the security of medical records, including a system "to ensure the integrity of the authentication and protect the security of all

[49] *See* New York Civil Rights Law § 79-l.

[50] *Id*., § 79-j; New York Public Health Law § 18(1)(e); Mental Hygiene Law § 33.13.

[51] *See* NY eHealth Collaborative Privacy & Security Minor Consent Tiger Team, *Barriers to the Exchange of Pediatric Health Information*, pp. 7-8 (July 2, 2010) (describing numerous state law provisions and state and federal case law that create confidentiality rights for minors seeking health care on their own).

[52] *See* New York Public Health Law Chapter 45, § 2306.

[53] *See* New York Public Health Law Chapter 45, Article 27-F.

[54] 10 NYCRR § 405.10 (a)(6).

[55] *See Williams v. Roosevelt Hospital*, 66 N.Y.2d 391 (1985).

transmissions, records and record entries" as well as implement policies to ensure the security of electronic or computer equipment from unwarranted access.[56]

I. Plaintiffs' & Class Members' Expectation of Privacy.

141. Plaintiffs and Class Members were aware of Defendant's duty of confidentiality when they sought medical services from Defendant.

142. Indeed, at all times when Plaintiffs and Class Members provided their PII/PHI to Defendant, they each had a reasonable expectation that the information would remain private, and that Defendant would not share the Private Information with third parties for a commercial purpose unrelated to patient care.

143. Plaintiffs' and Class Members' reasonable expectations of privacy in their PII/PHI are grounded in, among other things, Defendant's status as a healthcare provider, Defendant's common law obligation to maintain the confidentiality of patients' PII/PHI, state and federal laws protecting the confidentiality of medical information, state and federal laws protecting the confidentiality of communications and computer data, state laws prohibiting the unauthorized use and disclosure of personal means of identification, and Defendant's express and implied promises of confidentiality.

J. Defendant was Unjustly Enriched from the Use of The Pixel.

144. The primary motivation and a determining factor in Defendant's interception and disclosure of Plaintiffs' and Class Members' Private Information was to commit criminal and tortious acts in violation of federal and state laws as alleged herein, namely, the use of patient data for advertising in the absence of express written consent.

[56] 10 NYCRR § 405.10 (a)(2).

145. Defendant's further use of the Private Information after the initial interception and disclosure for marketing and revenue generation was in violation of HIPAA and an invasion of privacy. In exchange for disclosing its patients PII, Defendant is compensated by Facebook in the form of enhanced advertising services and more cost-efficient marketing on Facebook.

146. Upon information and belief, Defendant was advertising its services on Facebook, and the Pixel was used to "help [Defendant] understand the success of [its] advertisement efforts on Facebook."

147. Retargeting is a form of online marketing that targets users with ads based on their previous Internet communications and interactions.

148. Upon information and belief, Defendant re-targeted patients and potential patients to get more patients to use its services.

149. By utilizing the Pixel, the cost of advertising and retargeting was reduced, thereby benefitting Defendant.

REPRESENTATIVE PLAINTIFFS' EXPERIENCES

Plaintiff Ronda Cooper

150. As a condition of receiving Defendant's services, Plaintiff Cooper disclosed his Private Information to Defendant as recently as May 2023.

151. Plaintiff Cooper accessed Defendant's Website on his phone and computer to receive healthcare services from Defendant and at Defendant's direction. Plaintiff Cooper also accessed and used Mount Sinai's Patient Portal.

152. Plaintiff Cooper communicated with his doctor and requested virtual appointments via Defendant's Website and Patient Portal.

153. Plaintiff Cooper also disclosed information about his specific medical conditions and treatments sought to Defendant by using the Website.

154. Plaintiff Cooper has used and continues to use the same devices to maintain and access an active Facebook account throughout the relevant period in this case.

155. Plaintiff Cooper reasonably expected that his communications with Defendant via the Website and the Portal were confidential, solely between himself and Defendant and that such communications would not be transmitted to or intercepted by a third party.

156. Plaintiff Cooper provided his Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

157. As described herein, Defendant worked along with Facebook to intercept Plaintiff Cooper's communications, including those that contained Private and confidential information.

158. Defendant willfully facilitated these interceptions without Plaintiff Cooper's knowledge, consent or express written authorization.

159. Defendant transmitted to Facebook Plaintiff Cooper's FID, computer IP address, location and information such as treatment sought, appointment type, physician selected and button/menu selections.

160. By doing so without his consent, Defendant breached Plaintiff Cooper's right to privacy and unlawfully disclosed his Private Information.

161. After disclosing his private medical information to Defendant, Plaintiff Cooper began receiving targeted ads on his social media accounts such as Facebook, including those related to his medications, conditions, treatments and his specific medical diagnoses.

162. Defendant did not inform Plaintiff Cooper that it had shared his Private Information with Facebook.

163. Plaintiff Cooper suffered damages in, *inter alia*, the form of (i) invasion of privacy; (ii) violation of confidentiality of his Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages and (vi) the continued and ongoing risk to his Private Information.

164. Plaintiff Cooper has a continuing interest in ensuring that his Private Information is protected and safeguarded from future unauthorized disclosure.

Plaintiff Coral Fraser

165. As a condition of receiving Defendant's services, Plaintiff Fraser disclosed her Private Information to Defendant as recently as May 2022.

166. Plaintiff Fraser accessed Defendant's Website on her phone to receive healthcare services from Defendant and at Defendant's direction.

167. Plaintiff Fraser looked up doctors and specialty clinics on Defendant's Website.

168. Plaintiff Fraser also disclosed information about her specific medical conditions and treatments to Defendant by using the Website.

169. Plaintiff Fraser further submitted information regarding her personal zip code when she was searching for doctors on the "Find a Doctor" page.

170. Plaintiff Fraser has used the same device to maintain and access an active Facebook account throughout the relevant period in this case.

171. Plaintiff Fraser reasonably expected that her communications with Defendant via the Website were confidential, solely between herself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

172. Plaintiff Fraser provided her Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

173. As described herein, Defendant worked along with Facebook to intercept Plaintiff Fraser's communications, including those that contained Private and confidential information.

174. Defendant willfully facilitated these interceptions without Plaintiff Fraser's knowledge, consent or express written authorization.

175. Defendant transmitted to Facebook Plaintiff Fraser's FID, computer IP address, location, and information such as treatment sought, appointment type, physician selected and their specialty, and button/menu selections.

176. By doing so without her consent, Defendant breached Plaintiff Fraser's right to privacy and unlawfully disclosed Plaintiff Fraser's Private Information.

177. Defendant did not inform Plaintiff Fraser that it had shared her Private Information with Facebook.

178. After disclosing her private medical information to Defendant, Plaintiff Fraser began receiving targeted ads on her social media accounts such as Facebook and/or Instagram, including ads related to her specific conditions, treatments, and her medical diagnosis.

179. Plaintiff Fraser suffered damages in, *inter alia*, the form of (i) invasion of privacy; (ii) violation of confidentiality of her Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (vi) the continued and ongoing risk to her Private Information.

180. Plaintiff Fraser has a continuing interest in ensuring that her Private Information is protected and safeguarded from future unauthorized disclosure.

Plaintiff David Gitlin

181. As a condition of receiving Defendant's services, Plaintiff Gitlin disclosed his Private Information to Defendant as recently as September 2023.

182. Plaintiff Gitlin accessed Defendant's Website on his phone and computer to receive healthcare services from Defendant and at Defendant's direction. Plaintiff Gitlin also accessed and used Mount Sinai's Patient Portal.

183. Plaintiff Gitlin scheduled doctor's appointments for himself via Defendant's Website and Patient Portal.

184. Plaintiff Gitlin also disclosed information about his specific medical conditions and treatments sought to Defendant by using the Web Properties.

185. Plaintiff Gitlin has used the same devices to maintain and access an active Facebook account throughout the relevant period in this case.

186. Plaintiff Gitlin reasonably expected that his communications with Defendant via the Web Properties were confidential, solely between himself and Defendant and that such communications would not be transmitted to or intercepted by a third party.

187. Plaintiff Gitlin provided his Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

188. As described herein, Defendant worked along with Facebook to intercept Plaintiff Gitlin's communications, including those that contained Private and confidential information.

189. Defendant willfully facilitated these interceptions without Plaintiff Gitlin's knowledge, consent or express written authorization.

190. Defendant transmitted to Facebook Plaintiff Gitlin's FID, computer IP address, location and information such as treatment sought, appointment type, physician selected and button/menu selections.

191. By doing so without his consent, Defendant breached Plaintiff Gitlin's right to privacy and unlawfully disclosed his Private Information.

192. After disclosing his private medical information to Defendant, Plaintiff Gitlin began receiving targeted ads on his social media accounts such as Facebook, including those related to his medications, conditions, treatments and his specific medical diagnosis.

193. Defendant did not inform Plaintiff Gitlin that it had shared his Private Information with Facebook.

194. Plaintiff Gitlin suffered damages in, *inter alia*, the form of (i) invasion of privacy; (ii) violation of confidentiality of his Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages and (vi) the continued and ongoing risk to his Private Information.

195. Plaintiff Gitlin has a continuing interest in ensuring that his Private Information is protected and safeguarded from future unauthorized disclosure.

Plaintiff Gilbert Manda

196. As a condition of receiving Defendant's services, Plaintiff Manda disclosed his Private Information to Defendant as recently as September 2023.

197. Plaintiff Manda accessed Defendant's Website on his phone and computer to receive healthcare services from Defendant and at Defendant's direction. Plaintiff Manda also accessed and used Mount Sinai's Patient Portal.

198. Plaintiff Manda scheduled doctor's appointments for himself via Defendant's Website and the Patient Portal, searched for specialists, looked up his records and bills, and communicated with his providers.

199. Plaintiff Manda also disclosed information about his specific medical conditions and the treatments he sought to Defendant by using the Web Properties.

200. Plaintiff Manda has used and continues to use the same devices to maintain and access an active Facebook account throughout the relevant period in this case.

201. Plaintiff Manda reasonably expected that his communications with Defendant via the Website and the Portal were confidential, solely between himself and Defendant and that such communications would not be transmitted to or intercepted by a third party.

202. Plaintiff Manda provided his Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

203. As described herein, Defendant worked along with Facebook to intercept Plaintiff Manda's communications, including those that contained Private and confidential information.

204. Defendant willfully facilitated these interceptions without Plaintiff Manda's knowledge, consent or express written authorization.

205. Defendant transmitted to Facebook Plaintiff Manda's FID, computer IP address, location and information such as treatment sought, appointment type, physician selected, and button/menu selections.

206. By doing so without his consent, Defendant breached Plaintiff Manda's right to privacy and unlawfully disclosed his Private Information.

207. After disclosing his private medical information to Defendant, Plaintiff Manda began receiving targeted ads on his social media accounts such as Facebook, including those related to his medications, conditions, treatments and his specific medical diagnoses.

208. Defendant did not inform Plaintiff Manda that it had shared his Private Information with Facebook.

209. Plaintiff Manda suffered damages in, *inter alia*, the form of (i) invasion of privacy; (ii) violation of confidentiality of his Private Information; (iii) loss of benefit of the bargain;

(iv) diminution of value of the Private Information; (v) statutory damages and (vi) the continued and ongoing risk to his Private Information.

210. Plaintiff Manda has a continuing interest in ensuring that her Private Information is protected and safeguarded from future unauthorized disclosure.

TOLLING

211. Any applicable statute of limitations has been tolled by the "delayed discovery" rule. Plaintiffs did not know (and had no way of knowing) that their Private Information was intercepted and unlawfully disclosed because Defendant kept this information secret.

CLASS ACTION ALLEGATIONS

212. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated pursuant to Rule 23(b)(2), 23(b)(3) and 23(c)(4) of the Federal Rules of Civil Procedure.

213. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> All individuals residing in the United States whose Private Information was disclosed to a third party without authorization or consent through the third-party tracking technologies on Defendant's Website.

214. The New York sub-class that Plaintiffs seek to represent is defined as follows:

> All individuals residing in the State of New York whose Private Information was disclosed to a third party without authorization or consent through the third-party tracking technologies on Defendant's Website.

215. The Nationwide Class and the New York sub-class are collectively referred to herein as the "Classes." Excluded from the Classes are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or

director, any successor or assign and any Judge who adjudicates this case, including their staff and immediate family.

216. Plaintiffs reserve the right to modify or amend the definition of the proposed Classes before the Court determines whether certification is appropriate.

217. **Numerosity, Fed R. Civ. P. 23(a)(1).** The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are over one million individuals whose PII and PHI may have been improperly accessed by Facebook, and the Class is identifiable within Defendant's records. The majority of those Class Members are believed to be New York residents.

218. **Commonality & Predominance, Fed. R. Civ. P. 23(a)(2) and (b)(3).** Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the Plaintiffs and Class Members' Private Information;

b. Whether Defendant had duties not to disclose the Plaintiffs and Class Members' Private Information to unauthorized third parties;

c. Whether Defendant violated its privacy policy by disclosing Plaintiffs and Class Members' Private Information to Facebook, Meta or additional third parties.

d. Whether Defendant adequately, promptly and accurately informed Plaintiffs and Class Members that their Private Information would be disclosed to third parties;

e. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;

f. Whether Defendant adequately addressed and fixed the practices which permitted the disclosure of patient Private Information;

g. Whether Defendant engaged in unfair, unlawful or deceptive practices by failing to safeguard Plaintiffs and Class Members' Private Information;

h. Whether Defendant violated the consumer protection statutes invoked herein;

i. Whether Defendant knowingly made false representations as to its data security and/or privacy policy practices;

j. Whether Defendant knowingly omitted material representations with respect to its data security and/or privacy policy practices;

k. Whether Defendant's acts and practices violated Plaintiffs' and Class Members' privacy rights;

l. Whether Plaintiffs and Class Members are entitled to actual, consequential or nominal damages as a result of Defendant's wrongful conduct;

m. Whether Defendant knowingly made false representations as to it data security and/or privacy policy practices;

n. Whether Defendant knowingly omitted material representations with respect to its data security and/or privacy policy practices and

o. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of Defendant's disclosure of their Private Information.

219. **Typicality, Fed. R. Civ. P. 23(a)(3).** Plaintiffs' claims are typical of those of other Class Members because all had their Private Information compromised as a result of Defendant's use of the Meta Pixel, due to Defendant's misfeasance.

220. **Adequacy, Fed. R. Civ. P. 23(a)(4).** Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the members of the Class, and the infringement of the rights and the damages Plaintiffs have suffered are typical of other Class Members. Plaintiffs have also

retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

221. **Superiority and Manageability, Fed. R. Civ. P. 23(b)(3).** Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently and without the unnecessary duplication of evidence, effort and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against a defendant, like Northwell, with significant resources. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

222. **Policies Generally Applicable to the Class.** This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

223. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm

the limited resources of each individual Class member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs was exposed is representative of that experienced by the Class and will establish the right of each Class member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

224. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

225. **Ascertainability & Notice.** Membership in the Class can be determined by objective records maintained by Defendant, and adequate notice can be given to Class Members directly using information maintained in Defendant's records.

226. **Class-wide Injunctive Relief, Fed. R. Civ. P. 23(b)(2).** Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the practices complained of herein, and Defendant may continue to act unlawfully as set forth in this Complaint as Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

227. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would

advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to not disclose Plaintiffs' and Class Members' Private Information;

b. Whether Defendant owed a legal duty to not disclose Plaintiffs' and Class Members' Private Information with respect to Defendant's privacy policy;

c. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using and safeguarding their Private Information;

d. Whether Defendant failed to comply with its own policies, applicable laws, regulations and industry standards relating to data security;

e. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their Private Information would be disclosed to third parties;

f. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information disclosed to third parties;

g. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

NEW YORK LAW SHOULD APPLY TO PLAINTIFFS & THE CLASS AS A WHOLE

228. The State of New York has a significant interest in regulating the conduct of businesses operating within its borders.

229. New York, which seeks to protect the rights and interests of New York and all residents and citizens of the United States against a company headquartered and doing business in New York, has a greater interest in the claims of Plaintiffs and the Class than any other state and is most intimately concerned with the claims and outcome of this litigation.

230. The principal place of business and headquarters of Mount Sinai, located at One Gustave L. Levy Place, New York, NY 10029, is the "nerve center" of its business activities—the place where its high-level officers direct, control and coordinate Defendant's activities, including major policy decisions.

231. Defendant's actions and corporate decisions surrounding the allegations made in the Complaint were made from and in New York.

232. Defendant's breaches of duty to Plaintiffs and Class Members emanated from New York.

233. Application of New York law to the Class with respect to Plaintiffs' and Class Members' claims is neither arbitrary nor fundamentally unfair because New York has significant contacts and a significant aggregation of contacts that create a state interest in the claims of Plaintiffs and the Class.

234. Under New York's choice of law principles, which are applicable to this action, the common law of New York applies to the nationwide common law claims of all Class Members.

235. New York has a significant interest in regulating the conduct of businesses operating within its borders. New York also has the most significant relationship to Defendant, as it is headquartered in New York, its executives and officers are located in New York and the decisions giving rise to the allegations and claims asserted herein were made in New York. Thus, there is no conflict in applying New York law to non-resident consumers such as some of the potential Class Members.

COUNT I
Invasion of Privacy
(On Behalf of Plaintiffs & the Nationwide Class)

236. Plaintiffs and Class Members repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

237. Plaintiffs bring this claim individually and on behalf of the members of the Nationwide Class against Defendant.

238. Plaintiffs and Class Members had a reasonable expectation of privacy in their communications with Defendant via its Website and the communications platforms and services therein.

239. Plaintiffs and Class Members communicated sensitive and protected medical information and individually identifiable information that they intended for only Defendant to receive and that they understood Defendant would keep private.

240. Defendant's disclosure of the substance and nature of those communications to third parties without the knowledge and consent of Plaintiffs and Class Members is an intentional intrusion on Plaintiffs' and Class Members' solitude or seclusion.

241. Plaintiffs and Class Members had a reasonable expectation of privacy given Defendant's representations, its Notice of Privacy Practices and Privacy Policy.

242. Moreover, Plaintiffs and Class Members have a general expectation that their communications regarding healthcare with their healthcare providers will be kept confidential.

243. Defendant's disclosure of private medical information coupled with individually identifying information is highly offensive to the reasonable person.

244. As a result of Defendant's actions, Plaintiffs and Class Members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

245. Plaintiffs and Class Members have been damaged as a direct and proximate result of Defendant's invasion of their privacy and are entitled to just compensation, including monetary damages.

246. Plaintiffs and Class Members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiffs and Class Members for the harm to their privacy interests as a result of its intrusions upon Plaintiffs' and Class Members' privacy.

247. Plaintiffs and Class Members are also entitled to punitive damages resulting from the malicious, willful and intentional nature of Defendant's actions, directed at injuring Plaintiffs and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendant from engaging in such conduct in the future.

248. Plaintiffs also seek such other relief as the Court may deem just and proper.

COUNT II
Breach of Contract
(On behalf of Plaintiffs & the Nationwide Class)

249. Plaintiffs and Class Members repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

250. Defendant required Plaintiffs and Class Members to provide their Private Information, including names, email addresses, phone numbers, computer IP addresses, appointment information and other content submitted to Defendant's Website as a condition of their receiving healthcare services.

251. As a condition of utilizing Defendant's digital platforms and receiving services from Defendant, Plaintiffs and Class Members provided their Private Information and compensation for their medical care.

252. In so doing, Plaintiffs and Class Members entered into contracts with Defendant by which Defendant agreed to safeguard and protect such information, in its Privacy Policies and elsewhere, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and Class Members if their data had been breached and compromised or stolen.

253. Plaintiffs and Class Members fully performed their obligations under the contract with Defendant.

254. Defendant's relevant privacy policies and representations require it to take appropriate steps to safeguard the Private Information entrusted to it by the Plaintiffs and Class Members.

255. Defendant breached these agreements, which directly and/or proximately caused Plaintiffs and Class Members to suffer damages, including nominal damages.

256. Defendant breached the contracts it made with Plaintiffs and Class Members by failing to safeguard and protect their Private Information and by failing to provide timely and accurate notice to them that their Private Information was compromised as a result of Defendant sharing their Private Information with third parties without proper authorization.

257. As a direct and proximate result of Defendant's above-described breach of contract, Plaintiffs and Class Members have suffered (and will continue to suffer) the compromise and disclosure of their Private Information and identities.

258. As a direct and proximate result of Defendant's above-described breach of contract, Plaintiffs and Class Members are entitled to recover actual, consequential and/or nominal damages.

COUNT III
Breach of Fiduciary Duty
(On Behalf of Plaintiffs & the Nationwide Class)

259. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

260. A relationship existed between Plaintiffs and Class Members on the one hand and Defendant on the other in which Plaintiffs and Class Members put their trust in Defendant to protect their Private Information, and Defendant accepted that trust.

261. Defendant breached the fiduciary duty that it owed to Plaintiffs and Class Members by failing to act with the utmost good faith, fairness and honesty, failing to act with the highest and finest loyalty, and failing to protect, and intentionally disclosing, the Private Information of Plaintiffs and Class Members.

262. Defendant's breach of fiduciary duty was a legal cause of damage to Plaintiffs and Class Members.

263. But for Defendant's breach of fiduciary duty, the damage to Plaintiffs and Class Members would not have occurred.

264. Defendant's breach of fiduciary duty contributed substantially to producing the damage to Plaintiffs and Class Members.

265. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiffs and Class Members are entitled to and do demand actual, consequential and/or nominal damages, injunctive relief, and all other relief allowed by law.

COUNT IV
Unjust Enrichment
(On behalf of Plaintiffs & the Nationwide Class)

266. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

267. Plaintiffs assert this claim in the alternative to their contractual claims.

268. Defendant benefitted from Plaintiffs and Nationwide Class Members and unjustly retained those benefits at their expense.

269. Plaintiffs and Nationwide Class Members conferred a benefit upon Defendant in the form of Private Information that Defendant collected from Plaintiffs and Nationwide Class Members, without authorization and proper compensation. Defendant consciously collected and used this information for its own gain, providing Defendant with economic, intangible and other benefits, including substantial monetary compensation.

270. Defendant unjustly retained those benefits at the expense of Plaintiffs and Nationwide Class Members because Defendant's conduct damaged Plaintiffs and Class Members, all without providing any commensurate compensation to Plaintiffs and Class Members.

271. The benefits that Defendant derived from Plaintiffs and Nationwide Class Members were not offered by Plaintiffs and Class Members gratuitously and rightly belong to Plaintiffs and Class Members.

272. It would be inequitable under unjust enrichment principles in New York and every other state for Defendant to be permitted to retain any of the profit or other benefits wrongly derived from the unfair and unconscionable methods, acts and trade practices alleged in this Complaint.

273. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds that Defendant received and such other relief as the Court may deem just and proper.

COUNT V
Breach of Implied Contract
(On behalf of Plaintiffs & the Nationwide Class)

274. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

275. When Plaintiffs and Class Members provided their user data to Defendant in exchange for services, they entered an implied contract pursuant to which Defendant agreed to safeguard and not disclose their Private Information without consent.

276. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

277. Plaintiffs and Class Members would not have entrusted Defendant with their Private Information in the absence of an implied contract between them and Defendant obligating them not to disclose this Private Information without consent.

278. Defendant breached these implied contracts by disclosing Plaintiffs' and Class Members' Private Information to a third party, *i.e.*, Facebook.

279. As a direct and proximate result of Defendant's breaches of these implied contracts, Plaintiffs and Class Members sustained damages as alleged herein. Plaintiffs and Class Members would not have used Defendant's services, or would have paid substantially for these services, had they known their Private Information would be disclosed.

280. Plaintiffs and Class Members are entitled to compensatory and consequential damages because of Defendant's breach of implied contract.

COUNT VI
Breach of Confidence
(On behalf of Plaintiffs & the Nationwide Class)

281. Medical providers have a duty to their patients to keep non-public medical information confidential.

282. Plaintiffs and other Class Members had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged on Defendant's Web Properties, which were further buttressed by Defendant's express promises in its privacy policy.

283. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant installed its Pixel and CAPI to disclose and to transmit to third parties Plaintiffs' and other Class Members' communications with Defendant, including Private Information and the contents of such information.

284. These disclosures were made without Plaintiffs' or other Class Members' knowledge, consent or authorization.

285. The third-party recipients included, but were not limited to, Facebook.

286. The harm arising from a breach of provider-patient confidentiality includes erosion of the essential confidential relationship between the healthcare provider and the patient.

287. As a direct and proximate cause of Defendant's unauthorized disclosures of patient personally identifiable, non-public medical information and communications, Plaintiffs and other Class Members were damaged by Defendant's breach in that:

a. Sensitive and confidential information that Plaintiffs and Class Members intended to remain private is no longer private;

b. Plaintiffs and Class Members face ongoing harassment and embarrassment in the form of unwanted targeted advertisements;

c. Defendant eroded the essential confidential nature of the provider-patient relationship;

f. Defendant took something of value from Plaintiffs and Class Members and derived benefit therefrom without Plaintiffs' and Class Members' knowledge or informed consent and without compensation for such data;

g. Plaintiffs and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;

h. Defendant's actions diminished the value of Plaintiffs' and Class Members' Private Information; and

i. Defendant's actions violated the property rights Plaintiffs and Class Members have in their Private Information.

COUNT VII
Bailment
(On behalf of Plaintiffs & the Nationwide Class)

288. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

289. Defendant acquired and was obligated to safeguard the Private Information of Plaintiffs and Class Members.

290. Defendant accepted possession and took control of Plaintiffs' and Class Members' Private Information under such circumstances that the law imposes an obligation to safeguard the property of another.

291. Specifically, a constructive bailment arises when a defendant, as is the case here, takes lawful possession of the property of another and has a duty to account for that property, without intending to appropriate it.

292. Constructive bailments do not require an express assumption of duties and may arise from the bare fact of the thing coming into the actual possession and control of a person fortuitously or by mistake as to the duty or ability of the recipient to effect the purpose contemplated by the absolute owner.

293. During the bailment, Defendant owed a duty to Plaintiffs and Class Members to exercise reasonable care, diligence and prudence in protecting their Private Information.

294. Defendant breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiffs' and Class Members' Private Information, resulting in the unlawful and unauthorized access to, disclosure and misuse of such Information by third parties such as Facebook.

295. Defendant further breached its duty to safeguard Plaintiffs' and Class Members' Private Information by failing to notify them individually in a timely and accurate manner that their Private Information had been disclosed to third parties without Plaintiffs' and Class Members' knowledge, consent or authorization.

296. As a direct and proximate result of Defendant's breach of duty, Plaintiffs and Class Members have suffered compensable damages that were reasonably foreseeable to Defendant, including but not limited to, the damages set forth herein.

COUNT VIII
Violation of the New York Deceptive Trade Practices Act
New York Gen. Bus. Law § 349, *et seq.*
(On Behalf of Plaintiffs & the Nationwide Class and Alternatively on behalf of Plaintiffs & the New York sub-class)

297. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

298. By the acts and conduct alleged herein, Defendant committed unfair or deceptive acts and practices by:

a. promising to maintain the privacy and security of Plaintiffs' and Class Members' PHI as required by law;

b. installing the Facebook Pixel to operate as intended and transmit Plaintiffs' and Class Members' Private Information without their authorization to Facebook;

c. failing to disclose or omitting material facts to Plaintiffs and Class Members regarding the disclosure of their Private Information to Facebook;

d. failing to take proper action to ensure the Pixel was configured to prevent unlawful disclosure of Plaintiffs' and Class Members' Private Information;

e. unlawfully disclosing Plaintiffs' and Class Members' Private Information to Facebook.

299. These unfair acts and practices violated duties imposed by laws, including but not limited to, the Federal Trade Commission Act, HIPAA and NY GBL § 349.

300. Defendant's actions also constitute deceptive and unfair acts or practices because Defendant knew it failed to disclose to Plaintiffs and Class Members that their healthcare-related communications via the Web Properties would be disclosed to Facebook.

301. Defendant's actions also constitute deceptive and unfair acts or practices because Defendant intended that Plaintiffs and Class Members rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's offering of goods and services.

302. Specifically, Defendant was aware that Plaintiffs and Class Members depended and relied upon it to keep their communications confidential, and Defendant instead disclosed that information to Facebook.

303. In addition, Defendant's material failure to disclose that Defendant collects Plaintiffs' and Class Members' Private Information for marketing purposes with Facebook constitutes an unfair act or practice prohibited by the NY GBL § 349. Defendant's actions were immoral, unethical and unscrupulous.

304. Plaintiffs had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged at https://www.mountsinai.org and https://mychart.mountsinai.org/.

305. Plaintiffs' reasonable expectations of privacy in the communications exchanged with Defendant were further buttressed by Defendant's express promises in its Privacy Policy and HIPAA Privacy Notice.

306. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant deployed the Pixel to disclose and transmit Plaintiffs' personally identifiable, non-public medical information and the contents of her communications exchanged with Defendant to third parties, i.e., Facebook.

307. Defendant's disclosures of Plaintiffs' and Class Members' Private Information were made without their knowledge, consent, or authorization, and were unprivileged.

308. The harm arising from a breach of provider-patient confidentiality includes erosion of the essential confidential relationship between the healthcare provider and the patient.

309. Defendant willfully, knowingly, intentionally and voluntarily engaged in the aforementioned acts when it incorporated the Facebook Pixel with knowledge of the Pixel's purpose and functionality.

310. The harm described herein could not have been avoided by Plaintiffs and Class Members through the exercise of ordinary diligence.

311. As a result of Defendant's wrongful conduct, Plaintiffs were injured in that they never would have provided their PII and PHI to Defendant, or purchased Defendant's services, had they known or been told that Defendant shared their confidential and sensitive Private Information with Facebook.

312. As a direct and proximate result of Defendant's multiple, separate violations of the NY GBL § 349, Plaintiffs and Class member have suffered harm, including financial losses related to the payments or services made to Defendant that Plaintiffs and Class Members would not have made had they known of Defendant's disclosure of their PII and PHI to Facebook; lost control over the value of their PII and PHI; and other harm resulting from the unauthorized use or threat of unauthorized use of their PII and PHI, including for unwanted solicitations or marketing, entitling them to damages in an amount to be proven at trial.

313. Defendant's acts, practices and omissions were done in the course of Defendant's business of furnishing healthcare-related services to consumers in the State of New York.

314. Plaintiffs bring this action on behalf of herself and Class Members for the relief requested above and for the public benefit to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiffs, Class Members and the public from Defendant's unfair, deceptive and unlawful practices. Defendant's wrongful conduct, as alleged in this Complaint, has had widespread impact on the public at large.

315. As a result, Plaintiffs and Class Members are entitled to damages in an amount to be determined at trial, along with their costs and attorneys' fees incurred in this action.

COUNT IX
Violations of Electronic Communications Privacy Act ("ECPA")
18 U.S.C. § 2511(1) *et seq*.
Unauthorized Interception, Use and Disclosure
(On Behalf of Plaintiffs & the Nationwide Class)

316. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

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

318. 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.

319. The transmissions of Plaintiffs' PII and PHI to Defendant's Web Properties qualifies as a "communication" under the ECPA's definition of 18 U.S.C. § 2510(12).

320. **Electronic Communications**. The transmission of PII and PHI between Plaintiffs and Class Members and Defendant's Web Properties 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(2).

321. **Content.** The ECPA defines content, when used with respect to electronic communications, to "include [] *any* information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8).

322. **Interception.** The ECPA defines interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other

device" and "contents…include any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8).

323. **Electronic, Mechanical, or Other Device**. 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). The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. Plaintiffs' and Class Members' browsers;

b. Plaintiffs' and Class Members' computing devices;

c. Defendant's web-servers;

d. Defendant's Web Properties; and

e. The Pixel code deployed by Defendant to effectuate the sending and acquisition of patient communications.

324. By utilizing and embedding the Pixel on its Web Properties, Defendant intentionally intercepted, endeavored to intercept and procured another person to intercept, the electronic communications of Plaintiffs and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

325. Specifically, Defendant intercepted Plaintiffs' and Class Members' electronic communications via the Pixel, which tracked, stored and unlawfully disclosed Plaintiffs' and Class Members' PII to Facebook.

326. Defendant's intercepted communications include, but are not limited to, communications to/from Plaintiffs' and Class Members' regarding PII and PHI, treatment, medication and scheduling.

327. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiffs and Class Members 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).

328. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiffs and Class Members, 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).

329. **Unauthorized Purpose**. Defendant intentionally intercepted the contents of Plaintiffs' and Class Members' electronic communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any State—namely, invasion of privacy, among others.

330. Defendant intentionally used the wire or electronic communications to increase its profit margins. Defendant specifically used the Pixel to track and utilize Plaintiffs' and Class Members' PII and PHI for financial gain.

331. Defendant was not acting under color of law to intercept Plaintiffs and Class member's wire or electronic communication.

332. Plaintiffs and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiffs' privacy via the Pixel tracking code.

333. Any purported consent that Defendant received from Plaintiffs and Class Members was not valid.

334. In sending and in acquiring the content of Plaintiffs' and Class Members' communications relating to the browsing of Defendant's Web Properties, Defendant's purpose was tortious, criminal and designed to violate federal and state legal provisions, including as described above the following: (i) a knowing intrusion into a private, place, conversation, or matter that would be highly offensive to a reasonable person; and (ii) violation of NY GBL § 349.

COUNT X
Violation of ECPA Unauthorized Divulgence by Electronic Communications Service
18 U.S. Code § 2511(3)(a)
(On Behalf of Plaintiffs & the Nationwide Class)

335. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

336. The ECPA statute provides that "a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient." 18 U.S.C. § 2511(3)(a).

337. **Electronic Communication Service**. An "electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

338. Defendant's Web Properties are an electronic communication service, which provides users the ability to send or receive electronic communications. In the absence of Defendant's Web Properties, internet users could not send or receive communications regarding Plaintiffs' and Class Members' PII and PHI.

339. **Intentional Divulgence**. Defendant intentionally designed the Pixel tracking and was or should have been aware that, if misconfigured, it could divulge Plaintiffs' and Class Members' PII and PHI.

340. **While in Transmission**. Upon information and belief, Defendant's divulgence of the contents of Plaintiffs' and Class Members' communications was contemporaneous with their exchange with Defendant's Web Properties, to which they directed their communications.

341. Defendant divulged the contents of Plaintiffs' and Class Members' electronic communications without authorization. Defendant divulged the contents of Plaintiffs' and Class Members' communications to Facebook without Plaintiffs' and Class Members' consent and/or authorization.

342. **Exceptions do not apply**. In addition to the exception for communications directly to an electronic communications service ("ECS")[57] or an agent of an ECS, the ECPA states that "[a] person or entity providing electronic communication service to the public may divulge the contents of any such communication"

a. "as otherwise authorized in section 2511(2)(a) or 2517 of this title;"

b. "with the lawful consent of the originator or any addressee or intended recipient of such communication;"

c. "to a person employed or authorized, or whose facilities are used, to forward such communication to its destination;" or

d. "which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency."

[57] An ECS is "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

18 U.S.C. § 2511(3)(b).

343. Section 2511(2)(a)(i) provides:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

344. Defendant's divulgence of the contents of Plaintiffs' and Class Members' communications on Defendant's Web Properties to Facebook was not authorized by 18 U.S.C. § 2511(2)(a)(i) in that it was neither: (1) a necessary incident to the rendition of Defendant's service; nor (2) necessary to the protection of the rights or property of Defendant.

345. Section 2517 of the ECPA relates to investigations by government officials and has no relevance here.

346. Defendant's divulgence of the contents of user communications on Defendant's Web Properties through the Pixel was not done "with the lawful consent of the originator or any addresses or intend recipient of such communication[s]." As alleged above: (a) Plaintiffs and Class Members did not authorize Defendant to divulge the contents of their communications, and (b) Defendant did not procure the "lawful consent" from the websites or apps with which Plaintiffs and Class Members were exchanging information.

347. Moreover, Defendant divulged the contents of Plaintiffs' and Class Members' communications through the Pixel to individuals who are not "person[s] employed or whose facilities are used to forward such communication to its destination."

348. The contents of Plaintiffs' and Class Members' communications did not appear to pertain to the commission of a crime, and Defendant did not divulge the contents of their communications to a law enforcement agency.

349. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages; preliminary and other equitable or declaratory relief as may be appropriate; punitive damages in an amount to be determined by a jury; and a reasonable attorney's fee and other litigation costs reasonably incurred.

COUNT XI
Violation of Title II of the Electronic Communications Privacy Act
18 U.S.C. § 2702, *et seq*.
(STORED COMMUNICATIONS ACT)
(On Behalf of Plaintiffs & the Nationwide Class)

350. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

351. The ECPA further provides that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1).

352. Defendant stores the content of Plaintiffs' and Class Members' communications on Defendant's Web Properties and files associated with it.

353. When Plaintiffs or Class Members make a Web Properties communication, the content of that communication is immediately placed into storage.

354. Defendant knowingly divulges the contents of Plaintiffs' and Class Members' communications through the Pixel.

355. **Exceptions Do Not Apply**. Section 2702(b) of the Stored Communication Act provides that an electronic communication service provider "may divulge the contents of a communication—"

a. "to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient."

b. "as otherwise authorized in Section 2517, 2511(2)(a), or 2703 of this title;"

c. "with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;"

d. "to a person employed or authorized or whose facilities are used to forward such communication to its destination;"

e. "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;"

f. "to the National Center for Missing and Exploited Children, in connection with a reported submission thereto under section 2258A."

g. "to a law enforcement agency, if the contents (i) were inadvertently obtained by the service provider; and (ii) appear to pertain to the commission of a crime;"

h. "to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency"; or

i. "to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies Section 2523."

356. Defendant did not divulge the contents of Plaintiffs' and Class Members' communications to "addressees," "intended recipients," or "agents" of any such addressees or intended recipients of Plaintiffs and Class Members.

357. Section 2517 and 2703 of the ECPA relate to investigations by government officials and have no relevance here.

358. Section 2511(2)(a)(i) provides:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

359. Defendant's divulgence of the contents of Plaintiffs' and Class Members' communications on Defendant's Web Properties to Facebook was not authorized by 18 U.S.C. § 2511(2)(a)(i) in that it was neither: (1) a necessary incident to the rendition of Defendant's services; nor (2) necessary to the protection of the rights or property of Defendant.

360. Defendant's divulgence of the contents of user communications on Defendant's Web Properties was not done "with the lawful consent of the originator or any addresses or intend recipient of such communication[s]." As alleged above: (a) Plaintiffs and Class Members did not authorize Defendant to divulge the contents of their communications, and (b) Defendant did not procure the "lawful consent" from the websites or apps with which Plaintiffs and Class Members were exchanging information.

361. Moreover, Defendant divulged the contents of Plaintiffs and Class Members' communications through the Pixel to individuals who are not "person[s] employed or whose facilities are used to forward such communication to its destination."

362. The contents of Plaintiffs' and Class Members' communications did not appear to pertain to the commission of a crime, and Defendant did not divulge the contents of their communications to a law enforcement agency.

363. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages; preliminary and other equitable or declaratory relief as may be appropriate; punitive damages in an amount to be determined by a jury; and a reasonable attorney's fee and other litigation costs reasonably incurred.

COUNT XII
Violation of the Computer Fraud and Abuse Act (CFAA)
18 U.S.C. § 1030, *et seq*.
(On Behalf of Plaintiffs & the Nationwide Class)

364. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

365. Plaintiffs' and Class Members' mobile devices are, and at all relevant times have been, used for interstate communication and commerce, and are therefore "protected computers" under 18 U.S.C. § 1030(e)(2)(B).

366. Defendant exceeded, and continues to exceed, authorized access to the Plaintiffs' and Class Members' protected computers and obtained information thereby, in violation of 18 U.S.C. § 1030(a)(2), (a)(2)(C).

367. Defendant's conduct caused "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value" under 18 U.S.C. § 1030(c)(4)(A)(i)(I), *inter alia*, because

of the secret transmission of Plaintiffs' and Class Members' private and personally identifiable data and content—including the Web Properties visitor's electronic communications with the Web Properties, including their mouse movements, clicks, keystrokes (such as text being entered into an information field or text box), URLs of web pages visited and other electronic communications in real-time ("Web Properties Communications"), which were never intended for public consumption.

368. Defendant's conduct also constitutes "a threat to public health or safety" under 18 U.S.C. § 1030(c)(4)(A)(i)(IV), due to the private and personally identifiable data and content of Plaintiffs' and Class Members' Web Properties Communications being made available to Defendant, Facebook, and/or other third parties without adequate legal privacy protections.

369. Accordingly, Plaintiffs and Class Members are entitled to "maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g).

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Ronda Cooper, Coral Fraser, David Gitlin and Gilbert Manda respectfully pray for judgment in their favor and against Defendant Mount Sinai as follows:

A. For an Order certifying this action as a Class action and appointing Plaintiffs as Class Representatives and Plaintiffs' counsel as Class Counsel;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

C. For equitable relief compelling Defendant to utilize

appropriate methods and policies with respect to consumer data collection, storage and safety, and to disclose with specificity the type of PII and PHI disclosed to third parties;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

E. For an award of actual damages, compensatory damages, statutory damages and statutory penalties, in an amount to be determined, as allowable by law;

F. For an award of punitive damages, as allowable by law;

G. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

H. Pre- and post-judgment interest on any amounts awarded; and

I. Such other and further relief as this Honorable Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs Ronda Cooper, Coral Fraser, David Gitlin and Gilbert Manda hereby demand that this matter be tried before a jury.

Date: October 27, 2023

Respectfully submitted,

s/: James J. Bilsborrow
James J. Bilsborrow (JB8204)
WEITZ & LUXENBERG, PC
700 Broadway
New York, NY 10003
(212) 558-5500
jbilsborrow@weitzlux.com

Elena A. Belov
New York Bar No. 4080891
David S. Almeida
New York Bar No. 3056520
ALMEIDA LAW GROUP LLC

849 W. Webster Avenue
Chicago, Illinois 60614
T: (312) 576-3024
E: david@almeidalawgroup.com
E: elena@almeidalawgroup.com

Attorneys for Plaintiffs & Putative Classes