IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NORTH CAROLINA
WESTERN DIVISION

LINDA MATTHIAE, on behalf of herself and all others similarly situated, Plaintiff, v. **WAKEMED HEALTH AND HOSPITALS,** Defendant.	Case No. Judge **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Linda Matthiae ("Plaintiff") brings this Class Action Complaint against WakeMed Health and Hospitals ("WakeMed" or "Defendant"), as an individual and on behalf of all others similarly situated ("Class Members"), and alleges, upon personal knowledge as to her own actions and her counsels' investigation, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiff brings this class action against Defendant for its knowing and willful disclosure of personally identifiable information and personal health information including the names, email addresses, phone numbers, computer IP addresses, emergency contact information, appointment information, allergy and medication information, and other content communicated by Defendant's patients through Defendant's website and patient portal (collectively referred to herein as "Private Information").

2. Defendant WakeMed is a 970-bed private, not-for-profit healthcare system based in Raleigh, North Carolina. WakeMed is accredited by The Joint Commission, which monitors and evaluates health care organizations according to the established state-of-the-art quality and

safety standards.[1] WakeMed is the largest health system in Wake County, North Carolina's largest county.[2]

3. Despite WakeMed's status as one of the largest healthcare providers in the country, WakeMed knowingly incorporated tracking software on its website that disclosed the Private Information of Plaintiff's and Class Members to an unauthorized third party without the knowledge or consent of Plaintiff and Class Members.

4. As a condition of receiving healthcare, and at Defendant's direction, Defendant's patients (i.e., Plaintiff and Class Members) entrust it with scores of sensitive, non-public Private Information. Unbeknownst to Plaintiff and Class Members, Defendant intentionally configured and implemented software known as a Tracking Pixel ("Pixel") to collect and transmit information from its website to third parties without consent, including information communicated in sensitive and presumptively confidential patient portals.

5. A pixel is a piece of code used to track a visitor to a website and measure the activity they take on a webpage. A pixel is a piece of code embedded on each page a visitor to the website views. The code captures vast amounts of information, such as the webpage name and how visitors interact with the page, including which buttons they click and the information they enter into form fields (which can include contact and medical information). Pixels also capture search queries, visitor IP addresses, and browser identifiers.

6. As a result of Defendant's knowing and willful incorporation of the Pixel on its website, Plaintiff and thousands other Class Members have had their most sensitive personal information disclosed and exposed by WakeMed. [3]

[1] https://www.wakemed.org/about-us/wakemed-by-the-numbers
[2] https://www.wakemed.org/about-us/
[3] https://www.wakemed.org/patients-and-visitors/patient-rights-and-privacy-policies/meta-pixel-privacy

7. In March 2018, WakeMed launched a campaign to connect more patients to the WakeMed MyChart patient portal that involved Facebook advertisements and a Meta (Facebook's parent company) Pixel placed on the WakeMed Health website to help monitor how patients use its website and the effectiveness of its outreach programs. A Pixel is commonly used by organizations to measure activity and experiences on their website. In this case, Defendant configured the Pixel to capture and allow Private Information to be transmitted to Meta from the WakeMed website and MyChart portal (the "Data Breach").[4]

8. Over four years later in June 2022, WakeMed disabled and removed the pixel and began an investigation to learn the extent of patient information it had transmitted to Facebook.[5]

9. Based on that investigation, WakeMed determined that certain Private Information of Plaintiff and Class Members was disclosed to Meta and Facebook, depending upon a user's activity within the WakeMed website and MyChart portal.[6]

10. Defendant did not disclose the Data Breach to patients until October 11, 2022, when it sent letters to Data Breach victims ("Notice of Data Breach Letter"). As a result, Plaintiff and Class Members have not been properly informed that their Private Information has been disclosed.

11. Healthcare providers like Defendant that collect and store Private Information have statutory, regulatory, contractual, and common law duties to safeguard that information and ensure it remains private and safe from disclosure to unauthorized parties.

12. Plaintiff and those similarly situated relied upon Defendant to maintain the security and privacy of the Private Information they entrusted to it. Plaintiff and Class Members reasonably

[4] *Id.*
[5] *Id.*
[6] *Id.*

expected and understood that Defendant would comply with its obligations to keep the Private Information secure and safe from unauthorized access and disclosure.

13. Plaintiff and Class Members would not have used Defendant's services or provided it with their Private Information had they known that Defendant would disclose that information to third parties without their knowledge or consent.

14. Defendant is responsible for allowing this Data Breach through its willful and knowing configuration and implementation of the tracking Pixel, its failure to implement and maintain reasonable safeguards to prevent the disclosure of Private Information, its unreasonable data policies, its failure to adequately train employees, and its failure to comply with industry-standard data security practices.

15. Plaintiff brings this action on behalf of all persons whose Private Information was compromised as a result of Defendant's choice to install the tracking Pixel on its website and patient portal and configure it to capture and transmit its patients' Private Information. Defendant's conduct violates federal and state statutes and is an egregious breach of the duty it owed its patients to keep their Private Information confidential and secure from unauthorized disclosure.

16. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' Private Information was maintained ass confidential, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding securing Private Information. As the result, Plaintiff's and Class Members' Private Information was compromised through disclosure to Meta, Facebook, and likely unknown and unauthorized

third parties. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

PARTIES

17. Plaintiff Linda Matthiae is a citizen of North Carolina, residing in Raleigh, North Carolina.

18. Defendant WakeMed Health and Hospitals is a corporation with its principal place of business at 3000 New Bern Avenue, Raleigh, North Carolina 27610.

JURISDICTION AND VENUE

19. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity.

20. The Eastern District of North Carolina has personal jurisdiction over Defendant named in this action because Defendant and/or its parents or affiliates are headquartered in this District and Defendant conducts substantial business in North Carolina and this District through its headquarters, offices, parents, and affiliates.

21. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

Background

22. Defendant operates a website, www.wakemed.org, that allows patients to find a doctor that specializes in a particular area of medicine, schedule appointments, research medical

conditions and procedures offered by Defendant and other healthcare related services. Defendant also encourages its patients to use its MyChart digital patient portal. Patients use the MyChart portal can access their medical records, view test results, request prescription refills, view their medical histories from other healthcare providers, fill out medical forms, check into appointments, and communicate with their healthcare provider.[7]

23. Unbeknownst to Plaintiff and Class Members, Defendant installed the tracking Pixel, not only on its website, but on the MyChart portal that patients use to communicate sensitive, non-public, personal and health information to Defendant. As implemented by Defendant, the tracking Pixel was configured to collect and transmit the Private Information of Plaintiff and Class Members to Facebook, Meta, and unknown third parties without the knowledge or consent of Plaintiff and Class Members.

24. Defendant had a duty to maintain the information provided to it by its patients as confidential and to protect Plaintiff's and Class Members' Private Information from disclosure to third parties.

25. Defendant's Notice of Privacy Practices ("Privacy Policy") represents that it, "takes the protection of your personal information seriously, and we are committed to protecting health information about you." Defendant further acknowledges that "Protected Health Information is information that may identify you and that relates to your past, present, or future physical or mental health or condition; the provision of health care products and services to you; or the payment for such services."[8]

26. Defendant's Privacy Policy reassures patients that, "WakeMed is required by law to maintain the privacy of your protected health information, to provide individuals with Notice of

[7] https://youtu.be/gRnGXB9sntY
[8] https://www.wakemed.org/assets/documents/regulatory/notice-of-privacy-english.pdf

our legal duties and privacy practices with respect to protected health information, and to abide by the terms described in this Notice."[9]

27. WakeMed represents that it is committed to "making sure that health information that identifies you is kept private."[10]

28. Defendant's Privacy Policy does not permit Defendant to use and disclose Plaintiff's and Class Members' Private Information for marketing purposes.

29. Defendant violated its own Privacy Policy by unlawfully disclosing Plaintiff's and Class Members' Private Information to Facebook, Meta, and likely other third parties.

The Data Breach

30. On or about October 11, 2022, Defendant sent Plaintiff and Class Members a Notice of Data Breach informing them that the Pixel it installed on its website had collected and transmitted "information entered into the MyChart patient portal and appointment scheduling page back to Facebook." Defendant further stated that the Private Information disclosed to Facebook included: email addresses, phone numbers, and other contact information; computer IP addresses; emergency contact information; information provided during online check-in, such as allergy or medication information; COVID vaccine statuses; and information about appointments, such as appointment types and dates, physicians, and the button or menus selected while using the MyChart portal. Defendant also acknowledged that information that patients entered into form fields or text boxes, which could include Social Security numbers and financial information, was also potentially disclosed to Facebook.[11]

[9] *Id.*
[10] *Id.*
[11] https://www.wakemed.org/about-us/news-and-media/wakemed-news-releases/wakemed-notifies-patients-of-potential-data-privacy-incident

31. If a patient is a Facebook user, the Pixel also connects the information it collects and transmits to the user's Facebook profile. Facebook's get started page for the Pixel clearly discloses that the Pixel "relies on Facebook cookies, which enable us to match your website visitors to their respective Facebook User accounts. Once matched, we can tally their actions in the Facebook Ads Manager so you can use the data to analyze your website's conversion flows and optimize your ad campaigns."[12] Accordingly, Defendant chose to incorporate code on its website knowing that the code was intended to specifically identify its patients to Facebook alongside their protected health information and geographic location.

32. There is a potential that more information was disclosed to Meta and Facebook during the four years data was submitted to Meta from Defendant's system without detection.

33. Healthcare organizations that collect and store Private Information have statutory, regulatory, contractual, and common law duties to safeguard that information and to ensure it remains private. Healthcare providers like Defendant have a fiduciary duty to keep the Private Information of their patients confidential and protected from disclosure and Defendant's knowing implementation of tracking software that collects and discloses Private Information to third parties and marketers is an egregious breach of that duty.

The Tracking Pixel

34. Facebook describes itself as a "real identity platform,"[13] meaning users are allowed only one account and must share "the name they go by in everyday life."[14] To that end, when

[12] https://developers.facebook.com/docs/meta-pixel/get-started
[13] Sam Schechner and Jeff Horwitz, *How Many Users Does Facebook Have? The Company Struggles to Figure It Out*, WALL. ST. J. (Oct. 21, 2021).
[14] FACEBOOK, COMMUNITY STANDARDS, PART IV INTEGRITY AND AUTHENTICITY, https://www.facebook.com/communitystandards/integrity_authenticity.

creating an account, users must provide their first and last name, along with their birthday and gender.[15]

35. In 2021, Facebook generated $117 billion in revenue.[16] Roughly 97% of that came from selling advertising space.[17]

36. Facebook sells advertising space by highlighting its ability to target users.[18] Facebook can target users so effectively because it surveils user activity both on and off its site.[19] This allows Facebook to make inferences about users beyond what they explicitly disclose, like their "interests," "behavior," and "connections."[20] Facebook compiles this information into a generalized dataset called "Core Audiences," which advertisers use to apply highly specific filters and parameters for their targeted advertisements.[21]

37. Advertisers can also build "Custom Audiences."[22] Custom Audiences enables advertisers to reach "people who have already shown interest in [their] business, whether they're loyal customers or people who have used [their] app or visited [their] website."[23] With Custom Audiences, advertisers can target existing customers directly, and they can also build a "Lookalike Audiences," which "leverages information such as demographics, interests, and behavior from

[15] FACEBOOK, SIGN UP, https://www.facebook.com/
[16] 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
[17] *Id.*
[18] FACEBOOK, WHY ADVERTISE ON FACEBOOK, https://www.facebook.com/business/help/205029060038706.
[19] FACEBOOK, ABOUT FACEBOOK PIXEL, https://www.facebook.com/business/help/742478679120153?id=1205376682832142.
[20] FACEBOOK, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting.
[21] FACEBOOK, EASIER, MORE EFFECTIVE WAYS TO REACH THE RIGHT PEOPLE ON FACEBOOK, https://www.facebook.com/business/news/Core-Audiences.
[22] FACEBOOK, ABOUT CUSTOM AUDIENCES, https://www.facebook.com/business/help/744354708981227?id=2469097953376494.
[23] FACEBOOK, AD TARGETING, HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting.

your source audience to find new people who share similar qualities."[24] Unlike Core Audiences, advertisers can build Custom Audiences and Lookalike Audiences only if they first supply Facebook with the underlying data. They can do so through two mechanisms: by manually uploading contact information for customers, or by utilizing Facebook's "Business Tools."[25]

38. As Facebook puts it, the Business Tools "help website owners and publishers, app developers and business partners, including advertisers and others, integrate with Facebook, understand and measure their products and services, and better reach and serve people who might be interested in their products and services."[26] Put more succinctly, Facebook's Business Tools are bits of code that advertisers can integrate into their website, mobile applications, and servers, thereby enabling Facebook to intercept and collect user activity on those platforms.

39. 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.[27] 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.[28] Advertisers can even create their own tracking parameters by building a "custom event."[29]

---

[24] Facebook, About Lookalike Audiences, https://www.facebook.com/business/help/164749007013531?id=401668390442328.
[25] FACEBOOK, CREATE A CUSTOMER LIST CUSTOM AUDIENCE, https://www.facebook.com/business/help/170456843145568?id=2469097953376494; Facebook, Create a Website Custom Audience, https://www.facebook.com/business/help/1474662202748341?id=2469097953376494.
[26] FACEBOOK, THE FACEBOOK BUSINESS TOOLS, https://www.facebook.com/help/331509497253087.
[27] *See* FACEBOOK, FACEBOOK PIXEL, ACCURATE EVENT TRACKING, ADVANCED, https://developers.facebook.com/docs/facebook-pixel/advanced/; *see also* FACEBOOK, BEST PRACTICES FOR FACEBOOK PIXEL SETUP, https://www.facebook.com/business/help/218844828315224?id=1205376682832142; FACEBOOK, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/.
[28] FACEBOOK, SPECIFICATIONS FOR FACEBOOK PIXEL STANDARD EVENTS, https://www.facebook.com/business/help/402791146561655?id=1205376682832142.
[29] FACEBOOK, ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, https://www.facebook.com/business/help/964258670337005?id=1205376682832142; *see also* FACEBOOK, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/.

40. One such Business Tool is the Facebook Tracking Pixel. Facebook offers this piece of code to advertisers, like WakeMed Health, to integrate into their website. As the name implies, the Facebook Pixel "tracks the people and type of actions they take."[30] 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 request sent to the host website, along with additional data that the Facebook Pixel is configured to collect. 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 websites—Defendant's own code, and Facebook's embedded code.

41. An example illustrates the point. Take an individual who navigates to Defendant's website and clicks on a tab. When that tab is clicked, the individual's browser sends a request to Defendant's server requesting that server to load the particular webpage. Because WakeMed utilizes the Facebook Pixel, Facebook's embedded code, written in JavaScript, sends secret instructions back to the individual's browser, without alerting the individual that this is happening. Facebook causes the browser to secretly duplicate the communication with WakeMed, transmitting it to Facebook's servers, alongside additional information that transcribes the communication's content and the individual's identity.

42. As acknowledged in the Notice of Data Breach letter, Defendant configured the tracking Pixel to collect and transmit a host of sensitive, non-public information, including, patients' names and contact information, the identities of their doctors, the nature of their medical appointments, the information they entered into form fields (e.g., medical histories, financial

[30] FACEBOOK, RETARGETING, https://www.facebook.com/business/goals/retargeting.

information, contact information, and Social Security numbers), vaccination statuses, and other presumptively confidential information that patients believed they communicating only to their healthcare provider through a secure patient portal.

43. After collecting and intercepting this information, Facebook processes it, analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences.

44. Through the Facebook Pixel, Defendant WakeMed shares its patients' identities and online activity, including personal information and search results related to their private medical treatment.

45. Plaintiff never consented, agreed, authorized, or otherwise permitted Defendant WakeMed to disclose her Private Information and assist with intercepting their communications. Plaintiff was never provided with any written notice that Defendant discloses its website users' protected health information, nor were they provided any means of opting out of such disclosures. Defendant nonetheless knowingly disclosed Plaintiff's protected health information to Meta, Facebook, and unauthorized entities.

46. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for legitimate healthcare purposes only, and to make only authorized disclosures of this information.

Plaintiff Linda Matthiae Experience

47. Plaintiff Linda Matthiae entrusted her Private Information to Defendant as a condition of receiving Defendant's healthcare services.

48. Plaintiff accessed Defendant's website to receive healthcare services from Defendant and at Defendant's direction. Plaintiff reasonably expected that her online

communications with WakeMed were confidential, solely between herself and WakeMed, and that such communications would not be transmitted to or intercepted by a third party.

49. Plaintiff provided her Private Information to Defendant and trusted that the information would be safeguarded according to internal policies and state and federal law.

50. At the time of the Data Breach, Defendant requested and retained Plaintiff's name, email address, phone number, computer IP address, and emergency contact information, appointment information, and other content submitted into Defendant's website.

51. Defendant transmitted to Facebook Plaintiff's email address, phone number, computer IP address, emergency contact information, and information such as appointment type and date, physician selected, button/menu selections, and/or content typed into free text boxes

52. On October 11, 2022, Defendant sent a Notice of Data Breach letter to Plaintiff, notifying her that Defendant improperly disclosed Plaintiff's Private Information to a third party in the Data Breach.

53. Plaintiff Matthiae is very careful about sharing her sensitive Private Information. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

54. Plaintiff Matthiae stores any documents containing her Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for her various online accounts.

55. Defendant WakeMed breached confidentiality and unlawfully disclosed Plaintiff's personally identifiable information and protected health information without her consent.

56. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's Private Information—a form of intangible property that Plaintiff entrusted to

Defendant, which was compromised in and as a result of the Data Breach. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety, emotional distress, and increased concerns for the loss of her privacy.

57. Plaintiff has a continuing interest in ensuring that Plaintiff's Private Information, which, upon information and belief, remain backed up in Defendant's possession, is protected, and safeguarded from future breaches.

CLASS ALLEGATIONS

58. Plaintiff brings this nationwide class action on behalf of herself and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

59. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> **All persons Defendant identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.**

60. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

61. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

62. Numerosity, Fed R. Civ. P. 23(a)(1): Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, roughly 495,000 individuals whose Private Information may have been improperly accessed in the Data Breach, and each Class member is apparently identifiable within Defendant's records.

63. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Class exists and predominates over any questions affecting only individual Class Members. These include:

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

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

c. Whether Defendant had duties not to use Plaintiff's and Class Members' Private Information for non-healthcare purposes;

d. Whether Defendant failed to adequately safeguard Plaintiff's and Class Members' Private Information;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

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

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the means by which the Data Breach occurred;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by disclosing Plaintiff's and Class Members' Private Information;

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

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

m. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

n. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

64. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their Private Information compromised as a result of the Data Breach, due to Defendant's misfeasance.

65. 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 Plaintiff's 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 Plaintiff.

66. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest

that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intend to prosecute this action vigorously.

67. 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 large corporations, like Defendant. 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.

68. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff 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 Plaintiff were 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.

69. 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 demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

70. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

71. Unless a Class-wide injunction is issued, Defendant may continue in their unlawful disclosure of the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

72. Further, 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.

73. 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 Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to

exercise due care in collecting, storing, using, and safeguarding their Private Information;

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

a. Whether a contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that contract;

b. Whether Defendant breached the contract;

c. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

d. Whether Defendant breached the implied contract;

e. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

f. Whether Defendant willfully or knowingly disclosed the Private Information compromised in the Data Breach;

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

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

COUNT I
INVASION OF PRIVACY
(On Behalf of Plaintiff and the Class)

74. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

75. Plaintiff brings this claim individually and on behalf of the members of the proposed Class against Defendant.

76. Plaintiff and Class Members have an interest in: (1) precluding the dissemination and/or misuse of their sensitive, confidential communications and protected health information; and (2) making personal decisions and/or conducting personal activities without observation, intrusion or interference, including, but not limited to, the right to visit and interact with their healthcare provider without being subjected to unauthorized disclosure of Private Information without Plaintiff's and Class Members' knowledge or consent.

77. At all relevant times, by using Facebook's tracking pixel to record and communicate patient's information alongside their confidential medical communications, Defendant WakeMed intentionally invaded Plaintiff's and Class Members' privacy rights.

78. Plaintiff and Class Members had a reasonable expectation that their communications, identities, health information and other data would remain confidential when using Defendant WakeMed's website.

79. Plaintiff and Class Members did not authorize Defendant WakeMed to record and transmit Plaintiff's and Class Members' private medical communications alongside their personally identifiable health information.

80. This invasion of privacy is serious in nature, scope, and impact because it relates to patients' private medical communications. Moreover, it constitutes an egregious breach of the societal norms underlying the privacy right. The disclosure of Plaintiff's and Class Member's Private Information is highly offensive to a reasonable person.

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

82. Plaintiff 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.

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

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

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

86. Accordingly, Plaintiff and Class Members seek all relief available for invasion of privacy claims.

COUNT II
BREACH OF CONTRACT
(On behalf of Plaintiff and the Class)

87. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

88. Defendant required Plaintiff and the Class Members to provide their Private Information, including their names, email addresses, phone numbers, computer IP addresses, and emergency contact information, appointment information, and other content submitted into Defendant's website.

89. As a condition of utilizing Defendant WakeMed's website and receiving services from Defendant, Plaintiff and the Class provided their Private Information. In so doing, Plaintiff

and the Class entered into contracts with Defendant by which Defendant agreed to safeguard and maintain such information as confidential. Defendant represented in its Privacy Policies and elsewhere, that it would keep such information secure and confidential, and that it would timely and accurately notify Plaintiff and the Class in the event that their Private Information had been disclosed to an unauthorized party.

90. Plaintiff and Class Members provided their Private Information and paid for Defendant's services. Plaintiff and the Class Members fully performed their obligations under the contract with Defendant.

91. Upon information and belief, the Privacy Policy of Defendant requires it to take appropriate steps to safeguard the Private Information entrusted to it by the Plaintiff and Class Members.

92. Defendant breached these agreements, which directly and/or proximately caused Plaintiff and Class Members to suffer substantial damages.

93. Defendant breached the contracts it made with Plaintiff and the Class by failing to safeguard and protect their Private Information from disclosure, and by failing to provide timely and accurate notice to them that the Private Information was compromised as a result of the Data Breach.

94. As a direct and proximate result of Defendant's above-described breach of contract, Plaintiffs and the Class have suffered (and will continue to suffer) the compromise and disclosure of their Private Information and identities. Plaintiff and Class Member have suffered harm, including financial losses related to the payments or services made to Defendant that Plaintiff and Class Members would not have made had they known of Defendant's disclosure of their Private Information to Facebook; lost control over the value of their Private Information; and other harm

resulting from the unauthorized use or threat of unauthorized use of their Private Information, including for unwanted solicitations or marketing, entitling them to damages in an amount to be proven at trial.

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

96. As a direct and proximate result of Defendant's above-described breach of contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT III
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Class)

97. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

98. A relationship existed between Plaintiff and the Class in which Plaintiff and the Class put their trust in WakeMed to protect the Private Information of Plaintiff and the Class and WakeMed accepted that trust.

99. Defendant WakeMed breached the fiduciary duty that it owed to Plaintiff and the Class 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 the Private Information of Plaintiff and the Class.

100. Defendant's willful and knowing disclosure of the Private Information of its patients was an egregious breach of its fiduciary duty owed to Plaintiff and Class Members.

101. Defendant's breach of fiduciary duty was a legal cause of damage to Plaintiff and the Class.

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

103. Defendant's breach of fiduciary duty contributed substantially to producing the damage to Plaintiff and the Class.

104. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiff is entitled to and demand actual, consequential, and nominal damages and injunctive relief.

COUNT IV
VIOLATION OF N.C.G.S. § 75-1.1, *ET SEQ*.
(On behalf of Plaintiff and the Class)

105. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

106. N.C. Gen. Stat. § 75-1.1. (the "NC UDTPA") declares unlawful "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce."

107. Defendant's conduct was in and affecting commerce and constitutes an unfair or deceptive trade practice under the NC UDPTA.

108. Specifically, Defendant's unlawful disclosure of Plaintiff's and Class Members' Private Information constitutes a per se violation of NC UDPTA.

109. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the offering of healthcare services through its digital platforms in violation of the NC UDPTA, including by: (i) unlawfully disclosing Plaintiff's and Class Members' Private Information to Facebook, Meta, and third parties; (ii) failing to disclose or omitting material facts to Plaintiff and Class Members regarding the disclosure of their Private Information to Facebook, Meta, and third parties; and (iii) failing to take proper action to ensure the proper pixel was configured to prevent unlawful disclosure of Plaintiff's and Class Members' Private Information.

110. Defendant's actions also constitute deceptive and unfair acts or practices because Defendant knowingly configured and implemented the Pixel and failed to disclose to Plaintiff and Class Members that their healthcare related communications via the website would be disclosed to Facebook, Meta, and third parties.

111. Defendant's actions also constitute deceptive and unfair acts or practices because Defendant intended that Plaintiff 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. Namely, Defendant knew that Plaintiff and Class Members depended and relied upon it to keep their communications confidential and Defendant instead disclosed that information to a third party.

112. In addition, Defendant's material failure to disclose that Defendant collects Plaintiff's and Class Members' Private Information for marketing purposes with Facebook constitutes an unfair act or practice prohibited by the NC UDPTA. Defendant's actions were immoral, unethical, and unscrupulous.

113. Plaintiff has a reasonable expectation of privacy in her communications exchange with Defendant, including communications exchanged in the MyChart Portal.

114. Plaintiff's reasonable expectation of privacy in the communications exchanged with Defendant were further buttressed by Defendant's express promises in its Notice of Privacy Practices and HIPAA Privacy notice.

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

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

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

118. 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.

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

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

121. As a direct and proximate result of Defendant's violations of the NC UDPTA, Plaintiff and Class Member have suffered harm, including financial losses related to the payments or services made to Defendant that Plaintiff and Class Members would not have made had they known of Defendant's disclosure of their Private Information to Facebook; lost control over the value of their Private Information; and other harm resulting from the unauthorized use or threat of unauthorized use of their Private Information, including for unwanted solicitations or marketing, entitling them to damages in an amount to be proven at trial.

122. Pursuant to N.C. Gen. Stat. § 75-16, § 75.16.1, Plaintiff requests damages, treble damages, punitive damages, and attorneys' fees in addition to all other relief allowed by law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiff as Class Representative and her 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 Plaintiff's and Class Members' Sensitive Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff 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 Private Information compromised during the Data Breach;

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 court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: October 28, 2022

Respectfully Submitted,

/s/ Scott C. Harris
Scott C. Harris
N.C. Bar No: 35328
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
900 W. Morgan Street
Raleigh, NC 27603
Telephone: (919) 600-5003
Facsimile: (919) 600-5035
sharris@milberg.com

Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
Fax: (865) 522-0049
gklinger@milberg.com

Terence R. Coates (pro hac vice forthcoming)
Jonathan T. Deters (pro hac vice forthcoming)
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Telephone: 513.651.3700
Facsimile: 513.665.0219
tcoates@msdlegal.com

Counsel for Plaintiff and Putative Class

ClassAction.org