IN THE UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF NORTH CAROLINA
WINSTON-SALEM DIVISION

KEITH DAVID ALLEN, KARYN COOK, DAYMOND COX, KEVIN CURRY, MEGHAN CURRY, DR. RICHARD NERO, DAVID NOVACK, CHERYL TAYLOR, FERNANDO VALENCIA, and NATALIE WELLS-REYES *on behalf of themselves and all others similarly situated*, Plaintiffs, v. NOVANT HEALTH, INC., Defendant.	Case No. 1:22-cv-00697-WO-JEP Consolidated with: 1:22-cv-00700-WO-JEP; 1:22-cv-00709-WO-JEP and 1:22-cv-00799-WO-JEP **JURY TRIAL DEMANDED**

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Keith David Allen, Karyn Cook, Daymond Cox, Kevin Curry, Meghan Curry, Dr. Richard Nero, David Novack, Cheryl Taylor, Fernando Valencia, and Natalie Wells-Reyes ("Plaintiffs") are each patients or former patients of Novant Health, Inc. ("Novant "or "Defendant"), who bring this class action against Defendant in its individual capacity and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions, their counsel's investigation, and upon information and belief as to all other matters, as follows:

1. This case arises from Defendant's intentional, reckless, and negligent disclosure of Plaintiffs' and Class Members' confidential and private medical information

to Meta Platforms, Inc., d/b/a Meta ("Facebook"), both of which benefitted from Defendant's marketing program at the expense of its patients' privacy.

2. Defendant has admitted in its public notice that it improperly disclosed personally identifiable information ("PII") and non-public personal health information ("PHI")[1] including, but not limited to, demographic information such as email address, phone number, computer IP address, and contact information entered into Emergency Contacts or Advanced Care Planning on Defendant's website; and information such as appointment type and date, physician selected, button/menu selections, and/or content typed into free text boxes on Defendant's website (collectively referred to as "Private Information").[2]

3. According to its report submitted to the United States Department of Health and Human Services, Defendant admits that the Private Information of at least 1,362,296 individuals was improperly and unlawfully disclosed to Facebook without their knowledge or consent.[3]

4. Prior to the disclosure, Defendant encouraged Plaintiffs and Class Members to use its digital tools, including MyChart, via its website, novantmychart.org ("My Chart" or "novantmychart.org"), to receive healthcare services, and Plaintiffs and Class Members

[1] This information is collectively referred to as "PII and PHI" or collectively, "Private Information."

[2] https://www.novanthealth.org/home/about-us/newsroom/press-releases/newsid33987/2672/novant-health-notifies-patients-of-potential-data-privacy-incident-.aspx (last visited Nov. 14, 2022).

[3] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Nov. 14, 2022).

did so with the reasonable understanding that Defendant would secure and maintain any PII and PHI as confidential.

5. At all times that Plaintiffs and Class Members visited and utilized Defendant's website and MyChart portal, they had a reasonable expectation of privacy that Private Information collected through Defendant's website and contained within the MyChart portal would remain secure and protected and only utilized for medical purposes.

6. Plaintiffs and Class Members provided Private Information to Defendant in order to receive medical services rendered and with the reasonable expectation that Defendant would protect their Private Information. Plaintiffs and Class Members relied on Defendant to secure and protect the Private Information and not disclose it to unauthorized third parties without their knowledge or consent.

7. Defendant further made expressed and implied promises to protect Plaintiffs' and Class Members' Private Information and maintain the privacy and confidentiality of communications that patients exchange with Defendant.

8. Defendant owed common law, contractual, statutory, and regulatory duties to keep Plaintiffs' and Class Members communications and medical information safe, secure, and confidential. Furthermore, by obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized disclosure.

9. Defendant, however, failed in its obligations and promises by utilizing the Facebook Pixel, described below, on its website knowing that such technology would transmit and share Plaintiffs' and Class Members' Private Information with unauthorized third parties.

10. Specifically, in May 2020, Defendant launched a promotional and marketing campaign to entice more patients to use Defendant's MyChart patient portal. Defendant's MyChart patient portal is a website that encourages patients to exchange communications to search for a doctor, learn more about their conditions and treatments, access medical records and test results and make appointments. Defendant's website also provides for access to patient medical records with MyChart.

11. In the course of this marketing campaign, Defendant intentionally installed the well-known Facebook tracking pixel (the "Pixel") on its website that secretly enabled the unauthorized transmission and disclosure of Plaintiffs' and Class Members' confidential medical information.

12. A pixel is a piece of code that "tracks the people and type of actions they take."[4] Pixels are routinely used to target specific customers by utilizing the data gathered through the pixel to build profiles for the purposes of retargeting and future marketing. Upon information and belief, Defendant utilized the Pixel data to improve and save costs on its marketing campaign, improve its data analytics, and attract new patients.

[4] FACEBOOK, RETARGETING, https://www.facebook.com/business/goals/retargeting (last visited Nov. 14, 2022).

13. Operating as designed, Defendant's tracking Pixel allowed the Private Information that Plaintiffs and Class Members submitted to Defendant to be unlawfully disclosed to Facebook.

14. For example, when Plaintiffs or a Class Member accessed Defendant's website hosting the tracking Pixel, the Facebook software directed Plaintiffs' or Class Members' browser to send a message to Facebook's servers. The information sent to Facebook by Defendant included the Private Information that Plaintiffs and Class Members submitted to Defendant's website, including but not limited to, the type and date of a medical appointment and physician. Such Private Information would allow a third party (e.g., Facebook) to know that a specific patient was seeking confidential medical care. This type of disclosure could also allow a third party to reasonably infer that a specific patient was treating for a specific type of medical condition such as cancer, pregnancy or AIDS.

15. 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.

16. While Defendant willfully and intentionally incorporated the tracking Pixel into its website as early as May of 2020, Defendant did not disclose to Plaintiffs or Class Members that it shared their sensitive and confidential communications via the website

with Facebook until August 12, 2022.[5] As a result, Plaintiffs and Class Members were unaware that their PII and PHI were being surreptitiously transmitted to Facebook as they communicated with their healthcare provider and logged into the MyChart portal.

17. Defendant breached its obligations and in one or more of the following ways: (i) failing to adequately review its marketing programs and web based technology to ensure the hospital website 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 Facebook Pixels; (v) failing to warn Plaintiffs and Class Members; and (vi) otherwise failing to design, and monitor its website in to maintain the confidentiality and integrity of patient PII and PHI.

18. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, (iii) loss of benefit of the bargain, (iv) diminution of value of the Private Information, (v) statutory damages, and (v) the continued and ongoing risk to their Private Information.

19. It is unknown without discovery whether the Private Information was further disseminated to additional third-party marketing companies (e.g., Google, Twitter, Bing, LinkedIn, HotJar, LifePerson, The Trade Desk, or Adobe) for the purposes of building

[5] *See supra* Fn. 1.

profiles and retargeting or to insurance companies to set rates; however, there has been at least one report from a putative class member experiencing an increase in targeted marketing related to confidential medical information.

20. Plaintiffs seek to remedy these harms and bring causes of action for (1) Invasion of Privacy, (2) Violation of North Carolina's Unfair and Deceptive Trade Practice Act (N.C. Gen. Stat. § 75-1.1, *et seq.*); (3) Unjust Enrichment; (4) Breach of Implied Contract; (5) Violation of the Wiretap Act (18 U.S.C. § 2510, *et seq.*); and (6) Breach of Confidence.

PARTIES

21. Plaintiff Keith David Allen is a natural person and citizen of North Carolina, residing in Charlotte, North Carolina (Mecklenburg County), where he intends to remain. According to a Notice he received from Defendant, Plaintiff Allen's Private Information was disclosed to Facebook without his knowledge or consent. On numerous occasions, from 2016 to present Plaintiff Allen accessed novantmychart.org on his mobile device and/or computer and used the website to look for health care providers. Plaintiff Allen has used and continues to use the same devices to maintain and access an active Facebook account throughout the relevant period in this case. Pursuant to the systematic process described herein, Novant assisted Facebook with intercepting Plaintiff Allen's communications, including those that contained personally identifiable information, protected health information, and related confidential information. Novant assisted these interceptions without Plaintiff Allen's knowledge, consent, or express written

authorization. By failing to receive the requisite consent, Defendant breached confidentiality and unlawfully disclosed Plaintiff Allen's personally identifiable information and protected health information.

22. Plaintiff Karyn Cook is a natural person and citizen of North Carolina, residing in Mint Hill, North Carolina (Mecklenburg County), where she intends to remain. According to a Notice she received from Defendant, Plaintiff Cook's Private Information was disclosed to Facebook without her knowledge or consent. On numerous occasions from in or around 2008-2009 to the present, Plaintiff Cook accessed novantmychart.org on her mobile device and/or computer and used the website to look for health care providers. Plaintiff Cook has used and continues to use the same devices to maintain and access an active Facebook account throughout the relevant period in this case. Pursuant to the systematic process described herein, Novant assisted Facebook with intercepting Plaintiff Cook's communications, including those that contained personally identifiable information, protected health information, and related confidential information. Novant assisted these interceptions without Plaintiff Cook's knowledge, consent, or express written authorization. By failing to receive the requisite consent, Defendant breached confidentiality and unlawfully disclosed Plaintiff Cook's personally identifiable information and protected health

23. Plaintiff Kevin Curry is a natural person and citizen of North Carolina, residing in Waxhaw, North Carolina, where he intends to remain. According to a notice he received from Defendant, Plaintiff Kevin Curry's Private Information was disclosed to

Facebook without his knowledge or consent. On numerous occasions, from 2012 to present, , Plaintiff Kevin Curry accessed novantmychart.org on his mobile device and/or computer and used the website to look for health care providers, schedule appointments, review and download medical records. Plaintiff Kevin Curry has used and continues to use the same devices to maintain and access an active Facebook account throughout the relevant period in this case. Pursuant to the systematic process described herein, Novant assisted Facebook with intercepting Plaintiff Kevin Curry's communications, including those that contained personally identifiable information, protected health information, and related confidential information. Novant assisted these interceptions without Plaintiff Kevin Curry's knowledge, consent, or express written authorization. By failing to receive the requisite consent, Defendant breached confidentiality and unlawfully disclosed Plaintiff Kevin Curry's personally identifiable information and protected health information.

24. Plaintiff Meghan Curry is a natural person and citizen of North Carolina, residing in Waxhaw, North Carolina, where she intends to remain. According to a notice she received from Defendant, Plaintiff Meghan Curry's Private Information was disclosed to Facebook without her knowledge or consent. On numerous occasions from 2017 to present, Plaintiff Meghan Curry accessed novantmychart.org on her mobile device and/or computer and used the website to look for health care providers, schedule appointments, review and download medical records. Plaintiff Meghan Curry has used and continues to use the same devices to maintain and access an active Facebook account throughout the

relevant period in this case. Pursuant to the systematic process described herein, Novant assisted Facebook with intercepting Plaintiff Meghan Curry's communications, including those that contained personally identifiable information, protected health information, and related confidential information. Novant assisted these interceptions without Plaintiff Meghan Curry's knowledge, consent, or express written authorization. By failing to receive the requisite consent, Defendant breached confidentiality and unlawfully disclosed Plaintiff Meghan Curry's personally identifiable information and protected health information.

25. Plaintiff Daymond Cox is a natural person and citizen of Texas, residing in Midlothian, Texas, (Ellis County) where he intends to remain. According to a Notice he received from Defendant, Plaintiff Cox's Private Information was disclosed to Facebook without his knowledge or consent. On numerous occasions from 2013 to the present, Plaintiff Cox accessed novantmychart.org on his mobile device and/or computer and used the website to look for health care providers, schedule appointments, review and download medical records. Plaintiff Cox has used and continues to use the same devices to maintain and access an active Facebook account throughout the relevant period in this case. Pursuant to the systematic process described herein, Novant assisted Facebook with intercepting Plaintiff Cox's communications, including those that contained personally identifiable information, protected health information, and related confidential information. Novant assisted these interceptions without Plaintiff Cox's knowledge, consent, or express written authorization. By failing to receive the requisite consent, Defendant breached

confidentiality and unlawfully disclosed Plaintiff Cox's personally identifiable information and protected health information.

26. Plaintiff Dr. Richard Nero is a natural person and citizen of North Carolina, residing in Raleigh, North Carolina (Wake County), where he intends to remain. According to a Notice he received from Defendant, Plaintiff Nero's Private Information was disclosed to Facebook without his knowledge or consent. On numerous occasions from roughly 2016 or 2017 to the present, Plaintiff Nero accessed novantmychart.org on his mobile device and/or computer and used the website to look for health care providers. Plaintiff Nero has used and continues to use the same devices to maintain and access an active Facebook account throughout the relevant period in this case. Pursuant to the systematic process described herein, Novant assisted Facebook with intercepting Plaintiff Nero's communications, including those that contained personally identifiable information, protected health information, and related confidential information. Novant assisted these interceptions without Plaintiff Nero's knowledge, consent, or express written authorization. By failing to receive the requisite consent, Defendant breached confidentiality and unlawfully disclosed Plaintiff Nero's personally identifiable information and protected health information.

27. Plaintiff David Novack is a natural person and citizen of South Carolina, residing in Rock Hill, South Carolina (York County), where he intends to remain. According to a Notice he received from Defendant, Plaintiff Novack's Private Information was disclosed to Facebook without his knowledge or consent. Plaintiff Novack has been a

patient of Novant since 2006. On numerous occasions from 2020 to 2022, Plaintiff Novack accessed novantmychart.org on his mobile device and/or computer and used the website to look for health care providers. Plaintiff Novack has used and continues to use the same devices to maintain and access an active Facebook account throughout the relevant period in this case. Pursuant to the systematic process described herein, Novant assisted Facebook with intercepting Plaintiff Novack's communications, including those that contained personally identifiable information, protected health information, and related confidential information. Novant assisted these interceptions without Plaintiff Novack's knowledge, consent, or express written authorization. By failing to receive the requisite consent, Defendant breached confidentiality and unlawfully disclosed Plaintiff Novack's personally identifiable information and protected health information.

28. Plaintiff Cheryl Taylor is a natural person and citizen of North Carolina, residing in Charlotte, North Carolina (Mecklenburg County), where she intends to remain. According to a Notice she received from Defendant, Plaintiff Taylor's Private Information was disclosed to Facebook without her knowledge or consent. On numerous occasions since 2016, and especially in 2022, Plaintiff Taylor used novantmychart.org and Novant's app on her mobile device and/or computer. She used the website to look for health care providers, schedule appointments, and review her medical records. Plaintiff Taylor has used and continues to use the same devices to maintain and access an active Facebook account throughout the relevant period in her case. Pursuant to the systematic process described herein, Novant assisted Facebook with intercepting Plaintiff Taylor's

communications, including those that contained personally identifiable information, protected health information, and related confidential information. Novant assisted these interceptions without Plaintiff Taylor's knowledge, consent, or express written authorization. By failing to receive the requisite consent, Defendant breached confidentiality and unlawfully disclosed Plaintiff Taylor's personally identifiable information and protected health information.

29. Plaintiff Fernando Valencia is a natural person and citizen of North Carolina, residing in Winston-Salem, North Carolina (Forsyth County), where he intends to remain. According to a Notice he received from Defendant, Plaintiff Valencia's Private Information was disclosed to Facebook without his knowledge or consent. On numerous occasions from in or around May 2020 to August 2022 and through the present, Plaintiff Valencia accessed novantmychart.org on his mobile device and/or computer and used the website to look for health care providers. Plaintiff Valencia has used and continues to use the same devices to maintain and access an active Facebook account throughout the relevant period in this case. Pursuant to the systematic process described herein, Novant assisted Facebook with intercepting Plaintiff Valencia's communications, including those that contained personally identifiable information, protected health information, and related confidential information. Novant assisted these interceptions without Plaintiff Valencia's knowledge, consent, or express written authorization. By failing to receive the requisite consent, Defendant breached confidentiality and unlawfully disclosed Plaintiff Valencia's personally identifiable information and protected health information.

30. Plaintiff Natalie Wells-Reyes is a natural person and citizen of North Carolina, residing in Mint Hill, North Carolina (Mecklenburg County), where she intends to remain. According to a Notice she received from Defendant, Plaintiff Wells-Reyes's Private Information was disclosed to Facebook without her knowledge or consent. On numerous occasions from in or around June or July of 2020 to the present, Plaintiff Wells-Reyes accessed novantmychart.org on her mobile device and/or computer and used the website to look for health care providers. Plaintiff Wells-Reyes has used and continues to use the same devices to maintain and access an active Facebook account throughout the relevant period in this case. Pursuant to the systematic process described herein, Novant assisted Facebook with intercepting Plaintiff Wells-Reyes's communications, including those that contained personally identifiable information, protected health information, and related confidential information. Novant assisted these interceptions without Plaintiff Wells-Reyes's knowledge, consent, or express written authorization. By failing to receive the requisite consent, Defendant breached confidentiality and unlawfully disclosed Plaintiff Wells-Reyes's personally identifiable information and protected health information.

31. Defendant Novant Health, Inc. is a North Carolina company with its principal place of business at 2085 Frontis Plaza Blvd., Winston-Salem, North Carolina 27103. Defendant is a three-state integrated network of physician clinics, outpatient centers and hospitals. Its network consists of more than 1,800 physicians and 35,000 employees at

more than 800 locations, including 15 medical centers and hundreds of outpatient facilities and physician clinics.[6]

32. Headquartered in Winston-Salem, North Carolina, Defendant advertises that it is committed to making healthcare remarkable for patients and communities, serving more than 5 million patients annually.

33. Defendant is a covered entity under the Health Insurance Portability and Accountability Ac 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

34. This Court has subject matter jurisdiction over this action 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, 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.

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

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

[6]https://www.novanthealth.org/Portals/92/novant_health/documents/media/2022_Media_kits/2022_Novant%20Health%20Fact%20Sheet_final.pdf (last visited Nov. 14 , 2022).

COMMON FACTUAL ALLEGATIONS

Defendant Improperly Disclosed Plaintiffs' and Class Members' Private Information

37. In May 2020, Defendant launched a marketing campaign to connect Plaintiffs and Class Members to Defendant's digital healthcare platform with the goal of increasing profitability.

38. To accomplish this, Defendant utilized Facebook advertisements and intentionally installed the Pixel on its website. The Pixel is a piece of code that Defendant commonly used to measure activity and experiences on their website.[7]

39. Through seeking and using Defendant's services as a medical provider, and utilizing the website services, including the My Chart portal, 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 secretly installed on its website.

40. Plaintiffs and Class Members did not intend or have any reason to suspect the Private Information would be shared with Facebook or that Defendant was tracking their every movement and disclosing same to Facebook when they entered highly sensitive information on Defendant's website and patient portal.

[7] *Id*.

41. Defendant did not disclose to or warn Plaintiffs or Class Members that Defendant used Plaintiffs' and Class Members' website submissions for Facebook's marketing purposes.

42. Defendant tracked Plaintiffs and Class Members' Private Information via the Facebook Pixel from at least May 2020 to June 17, 2022.

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

44. Defendant's unauthorized disclosure is not just limited to activity on the public website, but based on Defendant's notice letter, the disclosure also involved information contained within the highly sensitive and private MyChart portal, which requires a specific login.

45. Defendant's notice letter states:

> "You are receiving this notice because our records indicate that you logged into your MyChart account during the time frame that the pixel was active, and thus it is possible that your information may have been involved."

46. Based on Defendant's admissions and statements, and 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 website;

c. And Plaintiffs' and Class Members' medical appointments, location of

treatments, specific medical providers, and specific medical conditions and treatments.

d. Other sensitive and medical information contained within the MyChart portal.

47. Defendant deprived Plaintiffs and Class Members of their privacy rights when it: (1) implemented technology (i.e. Pixels) 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 Plaintiffs or Class Members and without obtaining their express written consent

Operation Source Code

48. Web browsers are software applications that allow consumers to exchange electronic communications over the internet.

49. Every website is hosted by a computer server through which the entity in charge of the website exchanges communications with Internet users via their web browsers.

50. The set of instructions that commands the browser is called the source code.

51. 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.

52. The third parties to whom the website transmits data through pixels or web bugs do not provide any substantive content relating to the user's communications. Instead, these third parties are typically procured to track user data and communications for marketing purposes.

53. The web bugs are tiny and camouflaged to purposefully remain invisible to the user.

54. Thus, without any knowledge, authorization, or action by a user, a website developer like Defendant can use its source code to commandeer the user's computing device, causing the device to contemporaneously and invisibly re-direct the users personally identifiable non-public medial information to third parties.

The Facebook Pixel

55. The Defendant secretly deployed the Pixel on its website in violation of its common law, contractual, statutory, and regulatory duties and obligations.

56. The Facebook Pixel, a marketing product, is a "piece of code" that allowed the Defendant to "understand the effectiveness of [their] advertising and the actions [patients] take on [their] site."[8] It also allowed the Defendant to optimize the delivery of ads, measure cross-device conversions, create custom audiences, learn about the website, and decrease advertising and marketing costs.[9]

---

[8] https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited Nov. 14, 2022)

[9] *Id.*

57. Most importantly, it allowed Defendant and Facebook to secretly track patients on Defendant's website and patient portal and intercept their communications with same.

Facebook's Platform and its Business Tools

58. Facebook operates the world's largest social media company.

59. In 2021, Facebook generated $117 billion in revenue.[10] Roughly 97% of that came from selling advertising space.[11]

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, including IP addresses.

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

62. Facebook then sells advertising space by highlighting its ability to target users.[12] Facebook can target users so effectively because it surveils user activity both on and off its site.[13] This allows Facebook to make inferences about users beyond what they explicitly disclose, like their "interests," "behavior," and "connections."[14] Facebook

[10] 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 Nov. 14, 2022)

[11] *Id.*

[12] FACEBOOK, WHY ADVERTISE ON FACEBOOK, https://www.facebook.com/business/help/205029060038706 (last visited Nov. 14, 2022) .

[13] FACEBOOK, ABOUT FACEBOOK PIXEL, https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited Nov. 14, 2022).

[14] FACEBOOK, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS,

compiles this information into a generalized dataset called "Core Audiences," which advertisers use to apply highly specific filters and parameters for their targeted advertisements.[15]

63. Indeed, Facebook utilizes the precise type of information disclosed by Defendant to identify, target, and market products and services to individuals.

64. Advertisers can also build "Custom Audiences."[16] Custom Audiences enable 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."[17] 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 your source audience to find new people who share similar qualities."[18] 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."[19]

---

https://www.facebook.com/business/ads/ad-targeting (last visited Nov. 14, 2022).

[15] FACEBOOK, EASIER, MORE EFFECTIVE WAYS TO REACH THE RIGHT PEOPLE ON FACEBOOK, https://www.facebook.com/business/news/Core-Audiences (last visited Nov. 14, 2022).

[16] FACEBOOK, ABOUT CUSTOM AUDIENCES, https://www.facebook.com/business/help/744354708981227?id=2469097953376494 (last visited Nov. 14, 2022).

[17] FACEBOOK, AD TARGETING, HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting (last visited Nov. 14, 2022).

[18] Facebook, About Lookalike Audiences, https://www.facebook.com/business/help/164749007013531?id=401668390442328 (last visited Nov. 14, 2022).

[19] FACEBOOK, CREATE A CUSTOMER LIST CUSTOM AUDIENCE,

65. 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."[20] 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.

66. 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.[21] 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

---

https://www.facebook.com/business/help/170456843145568?id=2469097953376494; Facebook, Create a Website Custom Audience https://www.facebook.com/business/help/1474662202748341?id=2469097953376494 (last visited Nov. 14, 2022).

[20] FACEBOOK, THE FACEBOOK BUSINESS TOOLS, https://www.facebook.com/help/331509497253087 (last visited Nov. 14, 2022).

[21] *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/ (last visited Nov. 14, 2022).

views or purchases.[22] Advertisers can even create their own tracking parameters by building a "custom event." [23]

67. One such Business Tool is the Facebook Pixel. Facebook offers this piece of code to advertisers, like Defendant, to integrate into their website. As the name implies, the Facebook Pixel "tracks the people and type of actions they take."[24] 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. 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.

68. An example illustrates the point. Take an individual who navigates to Defendant's website and clicks on a tab for "Women's Health." When that tab is clicked, the individual's browser sends a GET request to Defendant's server requesting that server to load the particular webpage. Because Novant utilizes the Facebook Pixel, Facebook's

---

[22] FACEBOOK, SPECIFICATIONS FOR FACEBOOK PIXEL STANDARD EVENTS, https://www.facebook.com/business/help/402791146561655?id=1205376682832142. (last visited Nov. 14, 2022)

[23] 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/. (last visited Nov. 14, 2022)

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

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 Novant, 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 website and entered, e.g., Advanced Care Planning or AIDS treatment on Defendant's website, their Private Information was transmitted to Facebook, including, but not limited to, appointment type and date, physician selected, specific button/menu selections, content typed into free text boxes, demographic information, email addresses, phone numbers, and emergency contact information. During the same transmissions, the website would also provide Facebook with the patient's Facebook ID, IP address and/or device ID or other the information they input into Novant's website, like their home address or phone number. This is precisely the type of information that HIPAA requires healthcare providers to de-anonymize to protect the privacy of patients.[25] The Plaintiffs' and Class Members identities could be easily determined based on the Facebook ID, IP address and/or reverse lookup from the collection of other identifying information that was improperly disclosed.

69. The Facebook Pixel also intercepts and transmits information that patients type into search boxes, e.g., "do I have covid" or forms that request confidential

[25] https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited Nov. 14, 2022)

information like patient contact information, medical histories, insurance and financial information, and Social Security numbers.

70. After intercepting and collecting this information, Facebook processes it, analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences. If the website visitor is also a Facebook user, Facebook will associate the information that it collects from the visitor with a Facebook ID that identifies their name and Facebook profile, i.e., their real-world identity. A user's Facebook Profile ID 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 Facebook Profile ID uniquely identifies an individual's Facebook account, Meta—or any other person—can use the Facebook Profile ID to quickly and easily locate, access, and view the user's corresponding Facebook profile. In other words, the Pixel allows Meta to know what video content one of its users viewed on Fandom's website.

Defendant's Privacy Policies and Promises

71. Defendant's privacy policies represent to Plaintiffs and Class Members that Defendant will keep Private Information private and confidential and they will only disclose Private Information under certain circumstances. [26]

---

26 https://www.novanthealth.org/Portals/92/Assets/Documents/Corporate/PDFs/Novant%20Health%20Notice%20of%20Privacy%20Policies%20for%20North%20Carolina.pdf (last visited Nov. 14, 2022).

72. Defendant publishes several privacy policies that represent to patients and visitors to its website that Novant will keep sensitive information confidential and that they will only disclose PII and PHI provided to it under certain circumstances, none of which apply here.

73. Defendant publishes a Patient Bill of Rights which tells patients that they have the right to "personal privacy" and "[p]rivacy, confidentiality and access to your medical information." Defendant also requires that patients "[s]hare as much information with us as possible about your health [and] medications."[27]

74. Defendant's separate Notices of Privacy Practices assure Plaintiffs and Class Members, "[w]e must protect the privacy of health information about you that can identify you." [28]

75. 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:

- To provide healthcare treatment to you;
- To obtain payment for services;
- For healthcare operations;
- To raise money for our organization;
- To remind you about appointments;

[27] Patient Bill of Rights | Novant Health
[28] *Id*.

- To tell you about treatment options;
- To our business associates;
- When it is required by law;
- For public health activities;
- For health oversight activities;
- For a legal proceeding;
- For law enforcement purposes;
- To a medical examiner or funeral director;
- For organ, eye, or tissue donation purposes;
- For medical research;
- To avoid a serious threat to health or safety;
- For specialized government functions; and
- For law enforcement custodial situations.

76. Defendant's privacy policy does not permit Defendant to use and disclose Plaintiffs' and Class Members' Private Information for marketing purposes.

77. Defendant also promises patients that, "In any situation other than those listed above, we may ask for your written authorization before we use or disclose your PHI."[29]

[29] *Id.*

78. Defendant also publishes a Patient Privacy HIPAA notice that specifically represents:

> We can only release your personal health information to those directly involved in providing your care; however, you have the right to grant access to your personal medical or billing information to other individuals or organizations of your choice. If you choose to do so, we require a written authorization.[30]

79. Defendant's privacy policy does not permit Defendant to use and disclose Plaintiffs' and Class Members' Private Information for marketing purposes. Defendant further promises patients that "[i]n any situation other than those listed above, we may ask for your written authorization before we use or disclose your PHI."[31]

80. Defendant violated its own privacy policy by unlawfully intercepting and disclosing Plaintiffs' and Class Members' Private Information to Facebook and third parties without adequately disclosing that it shared Private Information with third parties and without acquiring the specific patients' consent or authorization to share the Private Information.

Defendant Violated HIPAA Standards

81. Under Federal Law, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient, a potential patient, or household member of a patient for marketing purposes without the patients' express written authorization.[32]

---

[30] https://www.novanthealth.org/home/patients--visitors/patient-bill-of-rights/patient-privacy-hipaa.aspx (last visited Nov. 14, 2022).
[31] *Id.*
[32] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

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

83. 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:

> 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.[33]

84. 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).[34]

Defendant Violated Industry Standards

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

---

[33] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (last visited Nov. 3, 2022)

[34] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf (last visited Nov. 3, 2022)

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

87. 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)

88. 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 authorized surrogate when the individual lacks decision-making capacity about the purposes for which access would be granted.

89. 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 ethics guidelines for confidentiality.

Plaintiffs' and Class Members' Expectation of Privacy

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

91. Indeed, at all times when Plaintiffs and Class Members provided their PII and 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.

IP Addresses are Personally Identifiable Information

92. Defendant has admitted that through the use of the Pixel the following Private Information was improperly disclosed to Facebook:

- Computer IP addresses

93. An IP address is a number that identifies the address of a device connected to the Internet.

94. IP addresses are used to identify and route communications on the Internet.

95. IP addresses of individual Internet users are used by Internet service providers, websites, and third-party tracking companies to facilitate and track Internet communications.

96. Facebook tracks every IP address ever associated with a Facebook user.

97. Google also tracks IP addresses associated with Internet users.

98. Facebook, Google, and other third-party marketing companies track IP addresses for use of tracking and targeting individual homes and their occupants with advertising by using IP addresses.

99. Under HIPAA, an IP address is considered personally identifiable information:

a. HIPAA defines personally identifiable information 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 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).

100. Consequently, by Defendant's own admissions of disclosing IP addresses, Defendant acknowledges its business practices violated HIPAA and industry privacy standards.

Defendant was Enriched and Benefitted from the Use of The Pixel and Unauthorized Disclosures

101. The sole purpose of the use of the Facebook Pixel on Defendant's website was marketing and profits.

102. In exchange for disclosing the personally identifiable information of its patients, Defendant is compensated by Facebook in the form of enhanced advertising services and more cost-efficient marketing on Facebook.

103. Per Defendant's admission in its Notice Letter to Plaintiffs and Class Members, Defendant was advertising its services on Facebook, and the Pixel was used to "help [Defendant] understand the success of [its] advertisement efforts on Facebook."

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

105. Upon information and belief, as part of its marketing campaign, Defendant re-targeted patients and potential patients to "get more patients connected to the Novant Health My Chart portal."[35]

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

Plaintiff Keith David Allen's Experiences

107. Plaintiff Keith David Allen entrusted his Private Information to Defendant. As a condition of receiving Defendant's services, Plaintiff Allen disclosed his Private Information to Defendant.

108. Plaintiff Allen accessed Defendant's website to receive healthcare services from Defendant and at Defendant's direction.

109. Plaintiff Allen scheduled doctor's appointments for himself and his daughter via the Defendant's website.

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

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

[35] *Id.*

112. As described herein, Defendant worked along with Facebook to intercept Plaintiff Allen's communications, including those that contained Private and confidential information. Defendant willfully facilitated these interceptions without Plaintiff Allen's knowledge, consent, or express written authorization.

113. Defendant transmitted to Facebook Plaintiff Allen's Facebook ID, email address, phone number, computer IP address, and contact information entered into Emergency Contacts or Advanced Care Planning; and information such as appointment type and date, physician selected, button/menu selections, and/or content typed into free text boxes.

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

115. Defendant did not inform Plaintiff Allen that it had shared his Private Information with Facebook until on or around August 12, 2022.

116. Plaintiff Allen is diagnosed with a specific disease and submitted information to Defendant's website about scheduling medical appointments for his disease to Facebook.

117. Plaintiff Allen suffered damages in form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (v) the continued and ongoing risk to their Private Information.

118. Plaintiff Allen has a continuing interesting in ensuring that Plaintiff Allen's Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future unauthorized disclosure.

Plaintiff Karyn Cook's Experiences

119. Plaintiff Karyn Cook entrusted her Private Information to Defendant. As a condition of receiving Defendant's services, Plaintiff Cook disclosed her Private Information to Defendant.

120. Plaintiff Cook accessed Defendant's website to receive healthcare services from Defendant and at Defendant's direction.

121. Plaintiff Cook 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.

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

123. As described herein, Defendant worked along with Facebook to intercept Plaintiff Cook's communications, including those that contained Private and confidential information. Defendant willfully facilitated these interceptions without Plaintiff Cook's knowledge, consent, or express written authorization.

124. Defendant transmitted to Facebook Plaintiff Cook's Facebook ID, email address, phone number, computer IP address, and contact information entered into

Emergency Contacts or Advanced Care Planning; and information such as appointment type and date, physician selected, button/menu selections, and/or content typed into free text boxes.

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

126. Defendant did not inform Plaintiff Cook that it had shared her Private Information with Facebook until on or around August 12, 2022.

127. During the relevant time period, Plaintiff Cook received notices of unauthorized charges.

128. In November 2021, Wells Fargo notified her of a $300 unauthorized charge on her card.

129. In May of 2022, Lowes Home Improvement notified her of a $10,000 charge on her Wells Fargo account.

130. Plaintiff Cook suffered damages in form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (v) the continued and ongoing risk to their Private Information.

131. Plaintiff Cook has a continuing interest in ensuring that Plaintiff Cook's Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future unauthorized disclosure.

Plaintiff Daymond Cox's Experiences

132. Plaintiff Daymond Cox entrusted his Private Information to Defendant. As a condition of receiving Defendant's services, Plaintiff Cox disclosed his Private Information to Defendant.

133. Plaintiff Cox has accessed Defendant's website more than a hundred times to communicate with his healthcare providers, request appointments, check medications, pay bills, review medical records, download medical records, and request refills on his prescriptions. He did so at Defendant's direction.

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

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

136. As described herein, Defendant worked along with Facebook to intercept Plaintiff Cox's communications, including those that contained Private and confidential information. Defendant willfully facilitated these interceptions without Plaintiff Cox's knowledge, consent, or express written authorization.

137. Defendant transmitted to Facebook Plaintiff Cox's Facebook ID, email address, phone number, computer IP address, and contact information entered into Emergency Contacts or Advanced Care Planning; and information such as appointment

type and date, physician selected, button/menu selections, and/or content typed into free text boxes.

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

139. Defendant did not inform Plaintiff Cox that it had shared his Private Information with Facebook until on or around August 12, 2022.

140. Following the receipt of his notice letter, Plaintiff Cox spent significant time scrutinizing his accounts for fraudulent charges.

141. Following the disclosure of his Private Information, Plaintiff Cox experienced an increase in the amount of targeted advertising on Facebook and other websites related to specific medical conditions treated by Novant.

142. In early 2022, Plaintiff Cox experienced multiple fraudulent charges on his credit cards. As a result, the cards were cancelled and reissued, during which time Plaintiff Cox was without access to his funds.

143. Plaintiff Cox does not recall receiving any notification of data breach in the last 10 years from any company other than Novant.

144. Plaintiff Cox suffered damages in the form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (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.

145. Plaintiff Cox has a continuing interest in ensuring that Plaintiff Cox's Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future unauthorized disclosure.

Plaintiff Kevin Curry's Experiences

146. Plaintiff Kevin Curry entrusted his Private Information to Defendant. As a condition of receiving Defendant's services, Plaintiff Kevin Curry disclosed his Private Information to Defendant.

147. Plaintiff Kevin Curry accessed Defendant's website to receive healthcare services from Defendant and at Defendant's direction.

148. Plaintiff Kevin Curry reasonably expected that his communications with Defendant via the website were confidential, solely between himself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

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

150. As described herein, Defendant worked along with Facebook to intercept Plaintiff Kevin Curry's communications, including those that contained Private and confidential information. Defendant willfully facilitated these interceptions without Plaintiff Kevin Curry's knowledge, consent, or express written authorization.

151. Defendant transmitted to Facebook Plaintiff Kevin Curry's Facebook ID, email address, phone number, computer IP address, and contact information entered into

Emergency Contacts or Advanced Care Planning; and information such as appointment type and date, physician selected, button/menu selections, and/or content typed into free text boxes.

152. By doing so without Plaintiff Kevin Curry's consent, Defendant breached Plaintiff Kevin Curry's right to privacy and unlawfully disclosed Plaintiff Curry's Private Information.

153. Defendant did not inform Plaintiff Kevin Curry that it had shared his Private Information with Facebook until on or around August 12, 2022.

154. Plaintiff Kevin Curry suffered damages in form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (v) the continued and ongoing risk to their Private Information.

155. Plaintiff Kevin Curry has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future unauthorized disclosure.

Plaintiff Meghan Curry's Experiences

156. Plaintiff Meghan Curry has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future unauthorized disclosure.

157. Plaintiff Meghan Curry entrusted her Private Information to Defendant. As a condition of receiving Defendant's services, Plaintiff Megan Curry disclosed her Private Information to Defendant.

158. Plaintiff Meghan Curry accessed Defendant's website to receive healthcare services from Defendant and at Defendant's direction.

159. Plaintiff Meghan Curry 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.

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

161. As described herein, Defendant worked along with Facebook to intercept Plaintiff Meghan Curry's communications, including those that contained Private and confidential information. Defendant willfully facilitated these interceptions without Plaintiff Meghan Curry's knowledge, consent, or express written authorization.

162. Defendant transmitted to Facebook Plaintiff Meghan Curry's Facebook ID, email address, phone number, computer IP address, and contact information entered into Emergency Contacts or Advanced Care Planning; and information such as appointment type and date, physician selected, button/menu selections, and/or content typed into free text boxes.

163. By doing so without Plaintiff Meghan Curry's consent, Defendant breached Plaintiff Meghan Curry's right to privacy and unlawfully disclosed Plaintiff Curry's Private Information.

164. Defendant did not inform Plaintiff Meghan Curry that it had shared her Private Information with Facebook until on or around August 12, 2022.

165. Plaintiff Meghan Curry suffered damages in form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (v) the continued and ongoing risk to their Private Information.

166. Plaintiff Meghan Curry has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future unauthorized disclosure.

Plaintiff Dr. Richard Nero's Experiences

167. Plaintiff Dr. Richard Nero entrusted his Private Information to Defendant. As a condition of receiving Defendant's services, Plaintiff Nero disclosed his Private Information to Defendant.

168. Plaintiff Nero accessed Defendant's website to receive healthcare services from Defendant and at Defendant's direction.

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

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

171. As described herein, Defendant worked along with Facebook to intercept Plaintiff Nero's communications, including those that contained Private and confidential information. Defendant willfully facilitated these interceptions without Plaintiff Nero's knowledge, consent, or express written authorization.

172. Defendant transmitted to Facebook Plaintiff Nero's Facebook ID, email address, phone number, computer IP address, and contact information entered into Emergency Contacts or Advanced Care Planning; and information such as appointment type and date, physician selected, button/menu selections, and/or content typed into free text boxes.

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

174. Defendant did not inform Plaintiff Nero that it had shared his Private Information with Facebook until on or around August 12, 2022.

175. Plaintiff Nero suffered damages in form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences

of the Data Breach; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (v) the continued and ongoing risk to their Private Information.

176. Plaintiff Nero has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future unauthorized disclosure.

Plaintiff David Novack's Experiences

177. Plaintiff David Novack entrusted his Private Information to Defendant. As a condition of receiving Defendant's services, Plaintiff Novack disclosed his Private Information to Defendant.

178. Plaintiff Novack accessed Defendant's website to receive healthcare services from Defendant and at Defendant's direction.

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

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

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

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

182. Defendant transmitted to Facebook Plaintiff Novack's Facebook ID, email address, phone number, computer IP address, and contact information entered into Emergency Contacts or Advanced Care Planning; and information such as appointment type and date, physician selected, button/menu selections, and/or content typed into free text boxes.

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

184. Defendant did not inform Plaintiff Novack that it had shared his Private Information with Facebook until on or around August 12, 2022.

185. Following the receipt of his notice letter, Plaintiff Novack spent significant time scrutinizing his accounts for fraudulent charges.

186. Following the disclosure of his Private Information, Plaintiff Novack experienced an increase in the amount of medical related spam and/or phishing communications that he received. For example, on or about October 28, 2022, Plaintiff Novack received an unsolicited call from an unknown individual attempting to sell him medical insurance, during which the caller referenced a specific type of medical issue that Plaintiff Novack discussed with Novant through its patient portal.

187. Plaintiff Novack suffered damages in form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (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 their Private Information.

188. Plaintiff Novack has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future unauthorized disclosure.

Plaintiff Cheryl Taylor's Experiences

189. Plaintiff Cheryl Taylor entrusted her Private Information to Defendant. As a condition of receiving Defendant's services, Plaintiff Taylor disclosed her Private Information to Defendant.

190. Plaintiff Taylor regularly accessed Defendant's Novant MyChart patient portal and Novant's app since February 2022 to receive healthcare services from Defendant and at Defendant's direction.

191. Plaintiff Taylor 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.

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

193. As described herein, Defendant worked along with Facebook to intercept Plaintiff Taylor's communications, including those that contained private and confidential information. Defendant willfully facilitated these interceptions without Plaintiff Taylor's knowledge, consent, or express written authorization.

194. Defendant transmitted to Facebook Plaintiff Taylor's Facebook ID, email address, phone number, computer IP address, and contact information entered into Emergency Contacts or Advanced Care Planning; and information such as appointment type and date, physician selected, button/menu selections, and/or content typed into free text boxes.

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

196. Defendant did not inform Plaintiff Taylor that it had shared her Private Information with Facebook until on or around August 12, 2022.

197. Following the receipt of her notice letter, Plaintiff Taylor spent significant time scrutinizing her accounts and credit report for fraudulent charges.

198. Plaintiff Taylor pays Experian $4.95 per month for credit monitoring. Experian recently informed Plaintiff Taylor that "[her] personal info [was] exposed 93 times." Experian has suggested that this was related to a data breach.

199. Plaintiff Taylor does not recall receiving any notification of data breach in the last 10 years other than the one she received from Defendant.

200. Plaintiff Taylor suffered damages in form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (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.

201. Plaintiff Taylor has a continuing interest in ensuring that Plaintiff Taylor's Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future unauthorized disclosure.

Plaintiff Fernando Valencia's Experiences

202. Plaintiff Fernando Valencia entrusted his Private Information to Defendant. As a condition of receiving Defendant's services, Plaintiff Valencia disclosed his Private Information to Defendant.

203. Plaintiff Valencia accessed Defendant's website to receive healthcare services from Defendant and at Defendant's direction.

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

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

206. As described herein, Defendant worked along with Facebook to intercept Plaintiff Valencia's communications, including those that contained Private and confidential information. Defendant willfully facilitated these interceptions without Plaintiff Valencia's knowledge, consent, or express written authorization.

207. Defendant transmitted to Facebook Plaintiff Valencia's Facebook ID, email address, phone number, computer IP address, and contact information entered into Emergency Contacts or Advanced Care Planning; and information such as appointment type and date, physician selected, button/menu selections, and/or content typed into free text boxes.

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

209. Defendant did not inform Plaintiff Valencia that it had shared his Private Information with Facebook until on or around August 12, 2022.

210. Following the receipt of his notice letter, he received a number of fraud alerts, unauthorized charges on his accounts, and unrelenting spam email, texts, and calls from May of 2022 through present.

211. Plaintiff Valencia received an alert that his Social Security number appeared on the "dark web."

212. In August of 2022, two unauthorized charges appeared on his Capital One account.

213. In September of 2022, an authorized charge appeared on his Wells Fargo account.

214. Plaintiff Valencia had to spend several hours resolving these issues.

215. In or around October of 2022, Plaintiff Valencia started receiving spam emails and seeing ads online regarding chiropractic care after a car wreck.

216. Plaintiff Valencia suffered damages in form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (v) the continued and ongoing risk to their Private Information.

217. Plaintiff Valencia has a continuing interest in ensuring that Plaintiff Valencia's PII and PHI, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future unauthorized disclosure.

Plaintiff Natalie Wells-Reyes's Experiences

218. Plaintiff Natalie Wells-Reyes entrusted her Private Information to Defendant. As a condition of receiving Defendant's services, Plaintiff Wells-Reyes disclosed her Private Information to Defendant.

219. Plaintiff Wells-Reyes accessed Defendant's website to receive healthcare services from Defendant and at Defendant's direction.

220. Plaintiff Wells-Reyes 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.

221. Plaintiff Wells-Reyes provided her Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

222. As described herein, Defendant worked along with Facebook to intercept Plaintiff Wells-Reyes's communications, including those that contained Private and confidential information. Defendant willfully facilitated these interceptions without Plaintiff Wells-Reyes's knowledge, consent, or express written authorization.

223. Defendant transmitted to Facebook Plaintiff Wells-Reyes's Facebook ID, email address, phone number, computer IP address, and contact information entered into Emergency Contacts or Advanced Care Planning; and information such as appointment type and date, physician selected, button/menu selections, and/or content typed into free text boxes.

224. By doing so without Plaintiff Wells-Reyes's consent, Defendant breached Plaintiff Wells-Reyes's right to privacy and unlawfully disclosed Plaintiff Wells-Reyes's Private Information.

225. Defendant did not inform Plaintiff Wells-Reyes that it had shared her Private Information with Facebook until on or around August 12, 2022.

226. In August of 2022, an unauthorized charge appeared on Plaintiff Wells-Reyes's Southeastern Employment Credit Union (SECU) account. After several hours of work and the inability to access her account's funds, she resolved this issue.

227. In October of 2022, medical conditions she had never been diagnosed with appeared in her Novant medical records inside the My Chart patient portal located at novantmychart.org.

228. Plaintiff Wells-Reyes began experiencing a marked increase in spam email, ads, and problems with her Facebook account at or around May or June of 2020 and continuing until present. Specifically, her Facebook was hacked in 2022, and she had to create a new Facebook account.

229. Plaintiff Wells-Reyes suffered damages in form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (v) the continued and ongoing risk to their Private Information.

230. Plaintiff Wells-Reyes has a continuing interest in ensuring that Plaintiff Wells-Reyes's Private Information, which, upon information and belief, remains backed up in Defendant's possession

231. Plaintiff Wells-Reyes has a continuing interest in ensuring that Plaintiff Wells-Reyes's PII and PHI, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future unauthorized disclosure.

TOLLING

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

CLASS ACTION ALLEGATIONS

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

234. 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 Pixel on Defendant's website and patient portal, including all persons receiving notice about such disclosures from Defendant.

235. Excluded from the Class 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.

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

237. Numerosity, Fed R. Civ. P. 23(a)(1). The Nationwide 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.

238. Commonality, 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 PII and PHI of Plaintiffs and Class Members;

b. Whether Defendant had duties not to disclose the PII and PHI of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendant violated its privacy policy by disclosing the PII and PHI of Plaintiffs and Class Members to Facebook, Meta, and/or additional third parties.

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

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

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

g. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiffs and Class Members;

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

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

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

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

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

239. Typicality, Fed. R. Civ. P. 23(a)(3). Plaintiffs' claims are typical of those of other Class Members because all had their PII and PHI compromised as a result of Defendant's incorporation of the Facebook Pixel, due to Defendant's misfeasance.

240. 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.

241. 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.

242. 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.

243. 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 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.

244. 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.

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

246. Unless a Class-wide injunction is issued, Defendant may continue in their 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.

247. 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.

248. 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 and 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.

249. Plaintiffs reserve the right to amend or modify the Class definition as this case progresses.

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

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

251. Plaintiffs and Class Members had a legitimate expectation of privacy regarding their PII and PHI and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

252. Defendant owed a duty to Plaintiffs and Class Members to keep their PII and PHI confidential.

253. The unauthorized disclosure and/or acquisition by a third party of Plaintiffs' and Class Members' PII and PHI is highly offensive to a reasonable person.

254. Defendant's willful and intentional disclosure of Plaintiffs' and Class Members' PII and PHI constitutes an intentional interference with Plaintiffs' and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

255. Defendant's conduct constitutes an intentional physical or sensory intrusion on Plaintiffs' and Class Members' privacy because Defendant facilitated Facebook's simultaneous eavesdropping and wiretapping of confidential communications.

256. Defendant failed to protect Plaintiffs' and Class Members' Private Information acted with a knowing state of mind when it incorporated the Facebook Pixel into its website because it knew the functionality and purpose of the Facebook Pixel.

257. Because Defendant intentionally and willfully incorporated the Facebook Pixel into its website and encouraged patients to use that website for healthcare purposes, Defendant had notice and knew that its practices would cause injury to Plaintiffs and Class Members.

258. As a proximate result of Defendant's acts and omissions, the private and sensitive PII and PHI of Plaintiffs and the Class Members was disclosed to a third party without authorization, causing Plaintiffs and the Class to suffer damages.

259. Plaintiffs, on behalf of themselves and Class Members, seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, loss of time and opportunity costs, punitive damages, plus prejudgment interest, and costs.

260. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their PII and PHI are still maintained by Defendant and still in the possession of Facebook and the wrongful disclosure of the information cannot be undone.

261. Plaintiffs and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not undo Defendant's disclosure of the information to Facebook who on information and belief continues to possess and utilize that information.

262. Plaintiffs, on behalf of themselves and Class Members, further seek injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiffs' and Class Members' PII and PHI and to adhere to its common law, contractual, statutory, and regulatory duties.

COUNT II
VIOLATION OF NORTH CAROLINA'S
UNFAIR & DECEPTIVE TRADE PRACTICES ACT
N.C. Gen. Stat. § 75-1.1, *et seq*.
(On behalf of Plaintiffs and the Nationwide Class)

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

264. 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."

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

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

267. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale and advertisement of their services in violation of the NC UDPTA by: (i) unlawfully disclosing Plaintiffs' and Class Members' Private Information to Facebook, Meta, and third parties; (ii) failing to disclose or omitting material facts to Plaintiffs 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 Plaintiffs' and Class Members' Private Information.

268. 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 website would be disclosed to Facebook, Meta, and third parties.

269. 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.

270. 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.

271. 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 NC UDPTA. Defendant's actions were immoral, unethical, and unscrupulous.

272. Plaintiffs had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged at www.novanthealth.org and on the log-in page for MyChart portal.

273. Plaintiffs' reasonable expectations of privacy in the communications exchanged with Defendant were further buttressed by Defendant's express promises in its Notice of Privacy Practices, Patient Bill of Rights and HIPAA Privacy notice.

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

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

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

277. 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.

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

279. 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.

280. As a direct and proximate result of Defendant's violations of the NC UDPTA, 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.

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

COUNT III
UNJUST ENRICHMENT
(On behalf of Plaintiffs and the Nationwide Class)

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

283. Defendant benefits from Plaintiffs and Class Members and unjustly retained those benefits at their expense.

284. Plaintiffs and Class Members conferred a benefit upon Defendant in the form of Private Information that Defendant collected from Plaintiffs and 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.

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

286. The benefits that Defendant derived from Plaintiffs and Class Members was not offered by Plaintiffs and Class Member gratuitously and rightly belongs to Plaintiffs and Class Members. It would be inequitable under unjust enrichment principles in North Carolina 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.

287. 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 IV
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and the Nationwide Class)

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

289. 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.

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

291. 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.

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

293. 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.

294. Plaintiffs and Class Members are entitled to compensatory and consequential damages as a result of Defendant's breach of implied contract.

COUNT V
VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA")
18 U.S.C. § 2511(1) *et seq*.
UNAUTHORIZED INTERCEPTION, USE, AND DISCLOSURE
(On Behalf of the Nationwide Class)

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

296. The ECPA protects both sending and receipt of communications.

297. 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.

298. The transmissions of Plaintiffs' PII and PHI to Defendant's website and/or MyChart portal qualifies as a "communication" under the ECPA's definition of 18 U.S.C. § 2510(12).

299. **Electronic Communications**. The transmission of PII and PHI between Plaintiffs and Class Members and Defendant's website and MyChart portal 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).

300. **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).

301. **Interception.** The ECPA defines the 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).

302. **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 MyChart portal; and

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

303. By utilizing and embedding the Pixel on its website, 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).

304. 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.

305. 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.

306. By intentionally disclosing or endeavoring to disclose the electronic communications of the 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).

307. 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).

308. **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.

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

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

311. 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.

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

313. In sending and in acquiring the content of Plaintiffs' and Class Members' communications relating to the browsing of Defendant's website, Defendant's purpose was tortious, criminal, and designed to violate federal and state legal provisions, including as described above the following: (1) a knowing intrusion into a private, place, conversation, or matter that would be highly offensive to a reasonable person; and (2) violation of NC UDPTA.

COUNT VI
VIOLATION OF ELECTRONIC COMMUNICATIONS PRIVACY ACT UNAUTHORIZED DIVULGENCE BY ELECTRONIC COMMUNICATIONS SERVICE
18 U.S. Code § 2511(3)(a)
(On Behalf of the Nationwide Class)

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

315. The ECPA Wiretap 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).

316. **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).

317. Defendant's website and/or MyChart portal are electronic communication services. Both services provide to users thereof the ability to send or receive electronic communications. In the absence of Defendant's website and MyChart portal, internet users could not send or receive communications regarding Plaintiffs' and Class Members' PII and PHI.

318. **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.

319. **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 website and/or MyChart portal, to which they directed their communications.

320. 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.

321. **Exceptions do not apply**. In addition to the exception for communications directly to an ECS or an agent of an ECS, the Wiretap Act 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."

18 U.S.C. § 2511(3)(b).

322. 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.

323. Defendant's divulgence of the contents of Plaintiffs' and Class Members' communications on Defendant's website and/or MyChart portal 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.

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

325. Defendant's divulgence of the contents of user communications on Defendant's browser through the Pixel code 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.

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

327. 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.

328. 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 VII
VIOLATION OF
TITLE II OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT
18 U.S.C. § 2702, *et seq*.
(STORED COMMUNICATIONS ACT)
(On Behalf of the Nationwide Class)

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

330. 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).

331. **Electronic Communication Service.** ECPA defines "electronic communications service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

332. Defendant intentionally procures and embeds various Plaintiffs' PII and PHI through the Pixel Code used on Defendant's website and/or MyChart portal, which qualifies as an Electronic Communication Service.

333. **Electronic Storage**. ECPA defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

334. Defendant stores the content of Plaintiffs' and Class Members' communications on Defendant's website and/or MyChart portal and files associated with it.

335. When Plaintiffs or Class Members make a website communication and/or submission to the MyChart portal, the content of that communication is immediately placed into storage.

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

337. **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 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."

338. 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.

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

340. 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.

341. Defendant's divulgence of the contents of Plaintiffs' and Class Members' communications on Defendant's website 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 the Defendant's services; nor (2) necessary to the protection of the rights or property of Defendant.

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

343. Defendant's divulgence of the contents of user communications on Defendant's website and/or MyChart portal 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.

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

345. 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.

346. 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 VIII
VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT (CFAA)
18 U.S.C. § 1030, *et seq.*
(On Behalf of Plaintiffs and the Nationwide Class)

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

348. The Plaintiffs' and the Class's 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).

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

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

351. 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 the Class being made available to Defendant, Facebook, and/or other third parties without adequate legal privacy protections.

352. Accordingly, Plaintiffs and the Class 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).

COUNT IX
BREACH OF CONFIDENCE
(On behalf of Plaintiffs and the Nationwide Class)

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

354. In North Carolina, medical providers have a duty to their patients to keep non-public medical information completely confidential.

355. Plaintiffs had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged on Defendant's website and on the log-in page for Defendant's MyChart portal.

356. Plaintiffs' reasonable expectations of privacy in the communications exchanged with Defendant were further buttressed by Defendant's express promises in its privacy policy.

357. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant deployed pixel code to disclose and transmit Plaintiffs' personally identifiable, non-public medical information, and the contents of their communications exchanged with Defendant to third parties.

358. The third-party recipients included, but were not limited to, Facebook and Meta.

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

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

361. As a direct and proximate cause of Defendant's unauthorized disclosures of patient personally identifiable, non-public medical information, and communications, Plaintiffs and 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. Defendant eroded the essential confidential nature of the provider-patient relationship;

c. General damages for invasion of their rights in an amount to be determined by a jury;

d. Nominal damages for each independent violation;

e. 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 compensating Plaintiffs for the data;

f. 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;

g. Defendant's actions diminished the value of Plaintiffs' and Class members' Personal Information; and

h. Defendant's actions violated the property rights Plaintiffs and Class members have in their Personal Information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Class and appointing Plaintiffs and their Counsel to represent such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members:

D. For an award of damages, including, but not limited to, actual, consequential, punitive, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

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

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

DATE: November 18, 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
gklinger@milberg.com

David K. Lietz*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Ave. NW, Suite 440
Washington, D.C. 20015-2052
Telephone: (866) 252-0878
Facsimile: (202) 686-2877
dlietz@milberg.com

Bryan L. Bleichner*
Philip J. Krzeski*
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone: (612) 339-7300
Fax: (612) 336-2940
bbleichner@chestnutcambronne.com
pkrzeski@chestnutcambronne.com

R. Michael Wells Jr. (N.C. Bar No: 33526)
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
7 Corporate Court, Suite B
Greensboro, NC 27408
Telephone: (916) 924-1829
Direct: (336) 970-3354
Fax: (916) 924-1289
mwells@justice4you.com

M. Anderson Berry*
Gregory Haroutunian*
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Facsimile: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com

Rachele R. Byrd*
Alex Tramontano*
WOLF HALDENSTEIN ADLER
FREEMAN & HERZ LLP
750 B Street, Suite 1820
San Diego, CA 92101
Telephone: (619) 239-4599
Facsimile: (619) 234-4599
byrd@whafh.com
tramontano@whafh.com

Terence R. Coates*
Jonathan T. Deters*
MARKOVITS, STOCK &
DEMARCO, LLC
119 E. Court St., Ste. 530
Cincinnati, Ohio 4502
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
jdeters@msdlegal.com

Joseph M. Lyon*
The Lyon Law Firm
2754 Erie Ave.
Cincinnati, Ohio 45208
Phone: (513) 381-2333
Fax: (513) 766-9011
jlyon@thelyonfirm.com

Counsel for Plaintiffs and the Putative Class

* *pro hac vice* forthcoming

CERTIFICATE OF SERVICE

I hereby certify that on November 18, 2022, a copy of the foregoing pleading was filed electronically with the Clerk of Court to be served by operation of the court's electronic filing system to all counsel of record.

/s/ Scott C. Harris
Scott C. Harris