COMMONWEALTH OF KENTUCKY

CASE NO._____
Electronically filed

JEFFERSON CIRCUIT COURT
DIVISION _____
JUDGE _____

RHONDA BLANDFORD, Individually, and as Mother and Next Friend of C.S., on behalf of herself, and all others similarly situated — **PLAINTIFF**

V. **CLASS ACTION COMPLAINT**

UOFL HEALTH, INC.

SERVE: James Rayome
Registered Agent
530 South Jackson Street
Louisville, Kentucky 40202

UNIVERSITY OF LOUISVILLE PHYSICIANS, INC. D/B/A UOFL PHYSICIANS

SERVE: VCT Services Louisville, LLC
2303 River Road, Suite 301
Louisville, Kentucky 40206 — **DEFENDANTS**

* * * * * * * * * * * *

Comes now the Plaintiff, RHONDA BLANDFORD, Individually, and as Mother and Next Friend of C.S. ("Blandford," "C.S.," or collectively, "Plaintiff"), on behalf of herself, and all others similarly situated, by and through counsel, and for her Class Action Complaint against the Defendants, UOFL HEALTH, INC., and UNIVERSITY OF LOUISVILLE PHYSICIANS, INC. d/b/a UOFL PHYSICIANS (collectively, "UofL Health" or "Defendants") alleges and states as follows:

I. INTRODUCTION

1. For years, a tracking tool installed on many hospitals' websites has been

collecting patients' highly sensitive Personally Identifying Information[1] and/or Protected Health Information[2] (collectively, "PHI") and sending it to Facebook.

2. The tracking tool is created by Facebook (now "Meta")[3] and is commonly known as "the Meta Pixel."

3. The Meta Pixel, by collecting patients' PII and PHI, collects information about patient's medical conditions, prescriptions, and doctor's appointments, in violation of state and federal laws.

4. UofL Health, a hospital and healthcare system in Louisville Metro., Jefferson County, Kentucky, despite knowing that the purpose of the Meta Pixel is to collect consumers' personal information, has been implementing the Meta Pixel on its hospital website and patient portal for years. By doing so, on information and belief, UofL Health has transmitted thousands of their patients' sensitive PHI to an unauthorized party—namely, Facebook—without its patients' consent, including Plaintiff and the proposed Class Members, in violation of its duty of confidentiality to its patients, and in violation of state and federal laws

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

[2] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, and its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 *Protected health information*. "Business Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, DEP'T FOR HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last accessed Apr. 16, 2020). UofL Health is clearly a "covered entity" and some of the data compromised in the Data Breach that this action arises out of is "protected health information," subject to HIPAA.

[3] Facebook changed its name from Facebook, Inc. to Meta Platforms, Inc. in October 2021. Plaintiff's reference to both "Facebook" and "Meta" throughout this complaint refer to the same company.

(the "Data Breach").

5. Despite knowing the risk that it was unlawfully transmitting patients' PHI, UofL Health chose to implement the Meta Pixel on its website and patient portal because it financially benefits Defendants. Specifically, UofL Health benefits from the ability to analyze its patients' experience and activity on its website to assess the website's functionality and traffic. UofL Health also gains information about its patients through the Meta Pixel that can be used to target them with advertisements as well as measure the results of advertisement efforts.

6. Because of UofL Health's actions, unauthorized parties now have access to UofL Health's patients' names, email addresses, phone numbers, other contact information, computer IP addresses emergency contact information, information provided during online check-in, medical information, information about upcoming appointments, and patient medical history.

7. As a direct and proximate result of the acts or omissions of UofL Health, set forth herein, Plaintiff and the proposed Class Members have suffered injury and damages, including but not limited to damages to, and diminution in the value of, their PII and PHI.

8. Plaintiff, Rhonda Blandford's daughter, C.S., a minor, is a patient of Defendants. And as a result, C.S. is now a data breach victim—her PII and PHI were exposed to unauthorized parties. Thus, Plaintiff brings this Class Action individually, and as Mother and Next Friend of C.S., on behalf of herself, and all others harmed by Defendants' misconduct.

II. PARTIES

9. Plaintiff, Rhonda Blandford is a natural person and citizen of the Commonwealth of Kentucky, with a principal residence in Louisville Metro., Jefferson County, Kentucky. She is the biological mother and Next Friend of her daughter, C.S., a

minor, and data breach victim.

10. Defendant, UofL Health, Inc., is a nonprofit corporation organized and existing under the laws of the Commonwealth of Kentucky with a principal business in Louisville Metro., Jefferson County, Kentucky at 530 South Jackson Street, Louisville, Kentucky 40202. James Rayome is Defendants' Registered Agent for service of process.

11. Defendant, University of Louisville Physicians, Inc., d/b/a UofL Physicians, is a nonprofit corporation organized and existing under the laws of the Commonwealth of Kentucky with a principal business in Louisville Metro., Jefferson County, Kentucky at 300 East Market Street, Suite 400, Louisville, Kentucky 40202. VCT Services Louisville, LLC, 2303 River Road, Suite 301, Louisville, Kentucky 40206 is UofL Physicians' Registered Agent for service of process.

III. JURISDICTION & VENUE

12. This Court has personal jurisdiction over UofL Health as Defendants is formed under Kentucky law, and as UofL Health's principal place of business is in the Commonwealth, such that it is at home within the Commonwealth.

13. The Court has subject matter jurisdiction pursuant to Kentucky Revised Statutes § 23A.010.

14. Venue is proper in Jefferson County under KRS § 452.460, because Defendants resides in Jefferson County.

IV. BACKGROUND FACTS

A. Defendants, UofL Health

15. UofL Health is a "fully integrated regional academic health system with more than 12,000 team members, seven hospitals, four medical centers, 200+ physician practice locations, 1,000+ providers, Frazier Rehab Institute, Brown Cancer Center and the Eye

Institute."[4]

16. UofL Health provides some medical services to patients through physicians' practices, UofL Physicians, including UofL Physicians – Neurology.[5]

17. Indeed, UofL Health prides itself for its:

> vast network of community and academic physicians [allowing it] to bring expertise, care and compassion to [] patients throughout Kentucky. As a leading academic health system, [it has] attracted specialists from every discipline—seasoned caregivers who have experience with a broad range of complex medical and surgical issues. This means [it] treat[s] the simplest medical issues with the same level of care and expertise as we do the more complex issues. Not only [does it] bring [its] knowledge to [its] patients, but [it] collaborate[s] with professionals throughout the country and in some cases the world, ensuring that [patients] have the right treatment options for whatever health issue [they] may be facing.[6]

18. On information and belief, Defendants collect and store highly sensitive PII and PHI on its systems of patients and visitors to its websites, including of Plaintiff and the proposed Class Members. Accordingly, Defendants assumes responsibility for safeguarding that information from unauthorized disclosures.

19. On information and belief, the PII and PHI that Defendants collect and store includes names, addresses, birth dates, insurance information, medical record numbers, patient account numbers, physician names, dates of service, diagnoses, treatment information, driver's license numbers, and Social Security numbers.

20. Defendants know that data security is important, and UofL Health maintains both a privacy policy for use of its website, https://uoflhealth.org/ ("Online Privacy Policy")[7] as well as a Notice of Privacy Practices.[8]

---

[4] https://uoflhealth.org/about/
[5] https://uoflhealth.org/services/neurology/
[6] https://uoflhealth.org/about/
[7] UofL Health, Inc., "Online Privacy Policy" https://uoflhealth.org/privacy-policy/ (last accessed March 19, 2023), **attached as Exhibit A.**
[8] UofL Health, Inc., "Notice of Privacy Practices" https://uoflhealth.org/wp-content/uploads/2022/01/UofL-Health-NPP-112019.pdf **attached as Exhibit B** (last accessed

21. UofL Health's Online Privacy Policy states:

> **What Information is Collected**
>
> We collect certain information from and about our website users directly from the user. When you submit a form we may ask you for your name, email address, and some other personal information. The more accurate information you volunteer, the better we are able to customize your experience.
>
> We may work with third-party service providers who may place third-party cookies, web beacons, or similar technologies on your computer as a visitor to our website to collect anonymous information about the use of our website. This information allows third-party's service providers to customize our content and advertising. **We do not permit these companies to collect any personal information about you using these technologies**.
>
> If you do not want these service providers to collect your information, please visit http://www.aboutads.info/choices to opt out of the various advertising technologies.[9]

22. UofL Health's Online Privacy Policy goes on to promise:

> **How We Protect Your Information**
>
> The privacy and protection of your personal information is vitally important to us. **UofL Health does not make personal information available to any third parties.** Any user statistics that we may provide to prospective partners regarding your usage of this website are provided in aggregate form and do not include any personally identifiable information about any individual user.[10]

23. In addition, UofL Health's Notice of Privacy Practices further enumerates the purposes for which it may disclose patients' PII and PHI, none of which include disclosure of this information to third-parties or Business Associates for "marketing" purposes, or specifically to Facebook.

24. UofL Health's Notice of Privacy Practices specifically promises that "[i]n these cases, we never share your information unless you give us written permission: Marketing purposes[;] Sale of your information [and] Most sharing of psychotherapy notes."[11]

March 19, 2023)

[9] https://uoflhealth.org/privacy-policy/ (emphasis added)

[10] *See Id.*

[11] Notice of Privacy Practices, Exhibit B.

25. In other words, UofL Health did not adequately inform its patients that any time a patient uses the patient portal or completes a simple transaction on the UofL Health website, the "passive information collection" of PII and/or PHI through the use of cookies and other technologies occurs, and then is then transferred to Facebook via the Metal Pixel.

B. Facebook's Meta Pixel

26. The Meta Pixel's primary purpose is for marketing and ad targeting.[12]

27. Meta's own website informs companies that "The Meta Pixel is a piece of code that you put on your website that allows you to measure the effectiveness of your advertising by understanding the actions people take on your website."[13]

28. According to Meta, the Meta Pixel can collect the following data:

> **Http Headers** – Anything present in HTTP headers. HTTP Headers are a standard web protocol sent between any browser request and any server on the internet. HTTP Headers include IP addresses, information about the web browser, page location, document, referrer and ***person using the website.*** (emphasis added).
> **Pixel-specific Data** – Includes Pixel ID and the Facebook Cookie.
>
> **Button Click Data** – Includes any buttons clicked by site visitors, the labels those buttons and any pages visited as a result of the button clicks.
>
> **Optional Values** – Developers and marketers can optionally choose to send additional information about the visit through Custom Data events. Example custom data events are conversion value, page type and more.
>
> **Form Field Names** – Includes website field names like email, address, quantity, etc., for when you purchase a product or service. We don't capture field values unless you include them as part of Advanced Matching or optional values.[14]

[12] *See Meta Pixel*, META FOR DEVELOPERS https://developers.facebook.com/docs/meta-pixel/ (last accessed Mar. 19, 2023).
[13] *About Meta Pixel*, Meta Business Help Center. https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last accessed Mar. 19, 2023).
[14] *Meta Pixel*, META FOR DEVELOPERS https://developers.facebook.com/docs/meta-pixel/ (last accessed Mar. 19, 2023).

29. Meta boasts to its prospective users that the Meta Pixel can be used to:

- **Make sure your ads are shown to the right people.** Find new customers, or people who have visited a specific page or taken a desired action on your website.

- **Drive more sales**. Set up automatic bidding to reach people who are more likely to take an action you care about, like making a purchase.

- **Measure the results of your ads.** Better understand the impact of your ads by measuring what happens when people see them.[15]

30. Meta likewise benefits from the data received from the Pixel and uses the data to serve targeted ads and identify users to be included in such targeted ads.

31. In June 2022, an investigation by The Markup[16] revealed that the Meta Pixel is embedded on the websites of 33 of the top 100 hospitals in the nation.[17] On those hospital websites, the Meta Pixel collects and sends Facebook a "packet of data," including sensitive personal health information, whenever a user interacts with the website, for example, by clicking a button to schedule a doctor's appointment.[18] The data is connected to an IP address, which is "an identifier that's like a computer's mailing address and can generally be linked to a specific individual or household—creating an intimate receipt of the appointment request for Facebook."[19]

32. In addition to the 33 hospitals identified by The Markup that had installed the Meta Pixel on their websites, The Markup identified seven health systems that had installed

[15] *About Meta Pixel*, Meta Business Help Center. https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last accessed Mar. 19, 2023).
[16] The Markup is a nonprofit newsroom that investigates how powerful institutions are using technology to change our society. *See* www.themarkup.org/about (last accessed Mar. 19, 2023).
[17] PIXEL HUNT, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites (last accessed Mar. 19, 2023).
[18] *Id.*
[19] *Id.*

the pixels inside their password-protected patient portals.[20]

33. David Holtzman, health privacy consultant and former senior privacy adviser in the U.S. Department of Health and Human Services' Office for Civil Rights, stated he was "deeply troubled" by what the hospitals were doing by capturing patient data and sharing it.[21]

34. On or about December 1, 2022, the United States Department of Health and Human Services, Office for Civil Rights ("HHS"), issued a bulletin, "Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates" ("HHS Bulletin").[22] As stated therein:

> Tracking technologies are used to collect and analyze information about how users interact with regulated entities' websites or mobile applications ("apps"). For example, a regulated entity may engage a technology vendor to perform such analysis as part of the regulated entity's health care operations. The HIPAA Rules apply when the information that regulated entities collect through tracking technologies or disclose to tracking technology vendors includes protected health information (PHI). Some regulated entities may share sensitive information with online tracking technology vendors and such sharing may be unauthorized disclosures of PHI with such vendors. **Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures[23] of PHI to tracking technology vendors or any other violations of the HIPAA Rules. For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.[24]**

---

[20] *Id.*
[21] *Id.*
[22] *See* U.S. Department for Health and Human Services, Office for Civil Rights, "Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates," available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last accessed Mar. 20, 2023).
[23] *See* U.S. Department for Health and Human Services, Office for Civil Rights, "Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates," available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last accessed Mar. 20, 2023), N.8 ("Regulated entities can use or disclose PHI, without an individual's written authorization, only as expressly permitted or required by the HIPAA Privacy Rule. *See* 45 CFR 164.502(a)."
[24] U.S. Department for Health and Human Services, Office for Civil Rights, "Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates," available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last accessed Mar. 20, 2023) (citations omitted) (emphases added); *see also*, *id.*, citing to 45 CFR

35. HHS's Bulletin further noted that the impermissible disclosure of PHI can cause myriad harm to individuals, including "identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI" and discloses highly-sensitive information regarding patients' diagnoses, and the nature, frequency and location of treatment.[25]

36. HHS's Bulletin cautioned that, "[w]hile it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI **only** as expressly permitted or required by the HIPAA Privacy Rule."[26]

37. HHS's Bulletin explained that, through tracking technologies such as Meta Pixel, covered entities disclose individual's information including PHI, provided when individuals use the entity's website or mobile applications, including medical records numbers, addresses, appointment dates, person's IP addresses or location, medical device IDs or unique identifying codes.[27]

38. The Bulletin further explained that "[a]ll such IIHI [individually identifiable health information] collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services."[28] This is because that

164.508(a)(3); 45 CFR 164.501 (definition of "Marketing").
[25] *Id*.
[26] *Id*.
[27] *Id*.
[28] *Id*.

information "connects the individual to the regulated entity […] and thus relates to the individual's past, present, or future health or health care or payment for care."[29]

39. Ultimately, in the Bulletin, HHS made clear that covered entities, such as UofL Health, must comply with HIPAA rules in connection with tracking technologies such as Meta Pixel, including but not limited to:[30]

- Ensuring that all disclosures of PHI to tracking technology vendors are specifically permitted by the Privacy Rule and that, unless an exception applies, only the minimum necessary PHI to achieve the intended purpose is disclosed.[33]

  - Regulated entities may identify the use of tracking technologies in their website or mobile app's privacy policy, notice, or terms and conditions of use.[34] However, the Privacy Rule does **not** permit disclosures of PHI to a tracking technology vendor based solely on a regulated entity informing individuals in its privacy policy, notice, or terms and conditions of use that it plans to make such disclosures. Regulated entities must ensure that all tracking technology vendors have signed a BAA and that there is an applicable permission prior to a disclosure of PHI.[35]

  - If there is not an applicable Privacy Rule permission or if the vendor is not a business associate of the regulated entity, then the individuals' HIPAA-compliant authorizations are required **before** the PHI is disclosed to the vendor. Website banners that ask users to accept or reject a website's use of tracking technologies, such as cookies, do **not** constitute a valid HIPAA authorization.

  - Further, it is insufficient for a tracking technology vendor to agree to remove PHI from the information it receives or de-identify the PHI before the vendor saves the information. Any disclosure of PHI to the vendor without individuals' authorizations requires the vendor to have a signed BAA in place **and** requires that there is an applicable Privacy Rule permission for disclosure.

40. Moreover, HIPPA rules require that covered entities using tracking technologies enter into a Business Associate Agreement with any tracking technology vendor that is a Business Associate.[31]

41. As articulated in HHS's Bulleting, covered entities utilizing tracking

[29] *Id.*
[30] *Id.*
[31] *See Id.*

technologies must also implement "administrative, physical, and technical safeguards" to protect transmitted PHI, such as appropriate encryption, authentication, and audit controls; and, must notify affected individuals and others of any impressible disclosure of PHI to tracking technology vendors who compromise that PHI. "In such instances, there is a presumption that there has been a breach of unsecured PHI unless the regulated entity can demonstrate that there is a low probability that the PHI has been compromised."[32]

42. On information and belief, UofL Health utilizes the Meta Pixel on its website, https://uoflhealth.org/, and transfers patient PII and/or PHI, including of Plaintiff and the proposed Class Members, to Facebook. While UofL represents in its Online Privacy Policy that the "user statistics" it provides to "prospective partners" regarding website usage are "provided in the aggregate form" without PII about individual users, in reality patient PII and PHI is transferred to Facebook by UofL Health without their authorization and consent.

43. Moreover, the YourAdChoices opt-out website referred to in UofL Health's Online Privacy Policy, http://www.aboutads.info/choices, displays Facebook, but states only that "**Use of Cookie Technologies for IBA:** Cookies are being used to customize ads for this browser."[33]

44. UofL Health's claimed use of providing website user statistics to its prospective partners, i.e., Facebook via the Metal Pixel, in the aggregate form without any PII of individual users, is not at all consistent with what Facebook has stated are the purposes of Meta Pixel: to collect individuals' information for ad targeting purposes.

45. Moreover, UofL Health is not just a "company," but a medical provider and therefore has heightened duties of care to its patients. UofL Health has been knowingly

[32] *Id.*
[33] *See* YourAdChoices, https://optout.aboutads.info/?c=2&lang=EN (last accessed Mar. 19, 2023) (emphasis added).

collecting its patients' PHI and PII and transmitting it to Facebook for an unknown period of time.

46. Here, UofL Health knew or should have known of the issuance of HHS's Bulletin in December 2022, and was on notice of the impropriety of its use of the Meta Pixel to transmit patient PII and PHI to Facebook without authorization in violation of HIPAA and attendant regulations.

C. Defendants Shared Plaintiff's and Class Members' Patient Data to Unauthorized Parties Without their Knowledge or Consent

47. Plaintiff's daughter, C.S., is a former and current patient of UofL Health, formerly receiving treatment in late 2020, approximately at UofL Health's Peace Hospital, and at UofL Physicians – Neurology.

48. When C.S. presented as a patient, Defendants required that she hand over her PII and PHI to UofL Health, in exchange for receiving psychiatric and neurological medical services. In doing so, UofL Health agreed to safeguard that data using reasonable means in accordance with state and federal law. Thus, Plaintiff expected that Defendants would take the steps necessary to secure C.S.'s sensitive, non-public data, PII and PHI.

49. Over the past three (3) years, since November 2020, approximately Plaintiff has used the UofL Health website to find a doctor and hospitals, including in connection with seeking mental health treatment for C.S. at Peace Hospital, or care for C.S. and UofL Physicians Neurology; to schedule an appointment; to search for treatment information; to search for physicians—including for C.S.'s neurological physician; to pay for medical services; to research treatment; and, through the patient portal.

50. Most recently, Plaintiff used the UofL Health website search function on or about March 18, 2023 to confirm the contact information for C.S.'s UofL Physicians neurologist.

51. In the above, Plaintiff has entrusted her and C.S.'s PII and/or PHI to UofL Health through its website.

52. Plaintiff and had no idea that UofL Health was collecting and using this data, including C.S.'s sensitive PII and PHI, and transmitting the same to third-party Facebook via the Meta Pixel, when she engaged with the UofL Health website that uses the Meta Pixel.

53. Plaintiff was certainly unaware that by using UofL Health's website and patient portal, Facebook was accessing C.S.'s PHI.

54. Plaintiff did not authorize UofL Health to transmit C.S.'s PII or PHI to Facebook or any other unauthorized party.

55. Defendants failed their patients—including C.S. For an unknown period of time, but on information and belief beginning at least as of November 18, 2020, approximately, to the present, Defendants transmitted Plaintiff C.S.'s PII and PHI at the Meta Pixel on its website https://uoflhealth.org/ and on the patient portal ("the Data Breach").

56. By placing the pixel on its website and patient portal, the pixel's software code transmitted information entered by patients, to Facebook. In other words, UofL Health's patients' highly sensitive personal information was exposed to Facebook, a party unauthorized to access such PHI.

57. UofL Health has entirely failed to properly inform its patients, including Plaintiff and the proposed Class Members, that their PII and/or PHI was being transferred to Facebook via the Meta Pixel.

58. Indeed, although UofL Health's mobile website informs visitors that the site wants to use their locations, it does not inform visitors that Meta Pixel is being used or give them the choice to opt-out.

59. Thus, Defendants kept their patients in the dark—thereby preventing them from taking swift remedial actions to protect themselves.

60. Defendants prioritized their own financial gain above their duty to protect patients' PHI. Defendants willingly engaged with Facebook to further its marketing and ad targeting goals to collect information. Defendants knew or should have known that the benefit to Facebook was to receiving patients' personal information for ad targeting.

D. Defendants Fail to Comply with Industry Standards.

61. The Federal Trade Commission ("FTC") has promulgated countless guides for businesses which stress the necessity of implementing reasonable data security practices. For one, the FTC explains that data security must be factored into all business decision-making.

62. In 2016, the FTC updated its cyber-security guide for businesses—*Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses.[34] The guidelines note that businesses should protect the personal patient information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problem.[35]

63. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[36]

64. The FTC brings enforcement actions against businesses for failing to adequately and reasonably protect patient data—treating the failure to employ reasonable

[34] Federal Trade Commission, Protecting Personal Information: A Guide for BUSINESS (2016),https://www.ftc.gov/system/files/documents/plain-language/pdf- 0136_proteting-personal-information.pdf.
[35] *Id*.
[36] *Id*.

and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

65. The FTC brings enforcement actions against healthcare providers like Defendants. For example, in *In the Matter of LabMD, Inc.*, the FTC found that Defendants' "data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act."[37]

66. Likewise, Defendants also failed to properly implement basic data security practices. Thus, Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

67. Defendants were always fully aware of their obligation to protect its patients' PII and PHI. Defendants was also aware of the significant repercussions that would result from its failure to do so.

68. Several best practices have been identified that at a minimum should be implemented by healthcare providers like Defendants. For example, healthcare providers should employ *at minimum* the following practices: employee cybersecurity education, strong passwords, multi-layer security (including firewalls, anti-virus, and anti-malware software), encryption (which makes data unreadable without a key), multi-factor authentication, data backups, and limiting which employees can access sensitive data.

69. Other best cybersecurity practices that are standard in the healthcare industry

[37] 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016).

include installing appropriate malware detection software, monitoring and limiting the network ports, protecting web browsers and email management systems, setting up network systems (like firewalls, switches, and routers), monitoring and protection of physical security systems, protecting against any possible communication system misuse, and training staff regarding critical points.

70. Defendants failed to meet the minimum standards of all the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC- 3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC)—which are all established standards for reasonable cybersecurity readiness.

71. These frameworks are applicable and current industry standards in healthcare. And Defendants failed to comply with these standards by transmitting its patients' PII and PHI to third parties without patients' knowledge or consent, thereby leaving the door wide open for the Data Breach—and the subsequent exposure and unauthorized access of patients' PII and PHI.

E. Defendants violated HIPAA Standards of Care by Transmitting PHI to an Unauthorized Third Party

72. HIPAA requires covered entities like Defendants to protect against reasonably anticipated threats to the security of sensitive patient health information.

73. Covered entities (including Defendants) must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

74. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other

things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI like the data Defendants left insufficiently guarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA.

75. 45 C.F.R. § 164.508 governs uses and disclosures of protected health information for which authorization is required. Under this rule, health care providers may not disclose protected health information without an authorization. Specifically enumerated under this provision as requiring authorization of a patient is "marketing":

> Authorization required: Marketing.
>
> (i) Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any use or disclosure of protected health information for marketing, except if the communication is in the form of:
>
> (A) A face-to-face communication made by a covered entity to an individual; or
>
> (B) A promotional gift of nominal value provided by the covered entity.

45 C.F.R. § 164.508(a)(3).

76. On information and belief, UofL Health does not comport with HIPPA and attendant rules in connection with its disclosure of patients' and/or web visitors' PII and PHI to Facebook via the Meta Pixel, including failing to obtain authorization from patients, including Plaintiff and the proposed Class Members, as required by 45 CFR § 164.508.

77. Data breaches—like Defendants'—are considered a "breach" under HIPAA because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of [PHI] in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." 45 C.F.R. 164.402

78. Data breaches—like Defendants' unauthorized disclosure here—are also

"security incidents" under HIPAA: A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. See the definition of security incident at 45 C.F.R. 164.304.

79. In short, the Data Breach occurred because Defendants provided unauthorized access and use of information to Facebook——demonstrating that they failed to comply with the safeguards and standards of care required by HIPAA regulations.

F. Plaintiff's Experience

80. Plaintiff, C.S., a minor, is a current patient of Defendants. And as a condition of receiving services, Plaintiff gave Defendants C.S.'s PII and PHI. In doing so, she trusted that Defendants would safeguard her information in accordance with industry standards, state law, and federal law.

81. UofL Health has failed to safeguard Plaintiff, C.S.'s personal information, including her PII and PHI, by transferring the same to Facebook via the Metal Pixel without authorization, in the Data Breach.

82. Plaintiff C.S.'s PII and/or PHI, received via the Meta Pixel, have been disclosed by UofL Health to Facebook, as evidenced by the new targeting of certain advertisements to Plaintiff's on Facebook corresponding to information transmitted to UofL Health via its websites.

83. Defendants have failed to inform Plaintiff and C.S. that her highly sensitive PII and PHI were unauthorizedly disclosed to Facebook via the Metal Pixel for marketing purposes.

84. Plaintiff and the proposed Class Members have suffered actual injury in the form of damages to and diminution in the value of their PII and PHI—a form of intangible

property that they entrusted to Defendants, which was ultimately compromised in the Data Breach.

85. As a result of Defendants' unauthorized transmittal of PII and PHI, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII and PHI is used;

b. The diminution in value of their PII and PHI;

c. The compromise and continuing publication of their PII and PHI; and,

d. Identity theft and fraudulent charges.

86. Plaintiff has spent—and will continue to spend—considerable time and effort monitoring her accounts to ensure that no unauthorized activity occurs as a result of the disclosure of their PII and PHI. Plaintiff fears for C.S.'s personal security, and she experiences uncertainty about the degree to which her sensitive information was exposed in the Data Breach.

87. Plaintiff has experienced—and will continue to experience—anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. Such injuries go far beyond mere allegations of worry or inconvenience. Rather, these injuries are precisely the type of harm (to a Data Breach victim) that the law contemplates and addresses.

88. Responsible for handling highly sensitive personal information (including healthcare information, financial information, and insurance information), Defendants knew or should have known the importance of safeguarding patients' personal information. Defendants also knew or should have known of the foreseeable consequences of a data breach. These consequences include the significant costs imposed on their patients due to the breach.

Still, Defendants failed to take adequate measures to prevent the Data Breach.

89. Because of Defendants' inadequate practices, the PII and PHI of Plaintiff, C.S., and members of the proposed Class were exposed to unauthorized third parties. In other words, Defendants opened up, disclosed, and then exposed patients' PII and PHI to third parties for marketing purposes.

V. CLASS ACTION ALLEGATIONS

90. Plaintiff, individually, and as Mother and Next Friend of C.S., sues on behalf of herself and the proposed Class ("Class"), defined as follows:

> All citizens of Kentucky whose PII and PHI was collected and transmitted by the Defendants to an unauthorized party using pixels.

Excluded from the Class are Defendants, their agents, employees, affiliates, parents, subsidiaries, any entity in which Defendants have a controlling interest, any Defendants officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

91. Plaintiff reserves the right to amend the class definition.

92. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of Class Members' claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims for each Class Member.

93. This action satisfies the requirements for a class action under CR 23.01 and CR 23.02(c), including requirements of numerosity, commonality, typicality, adequacy, predominance, and superiority:

a. **Numerosity**. Plaintiff is representative of the proposed Class, consisting of far too many members to join in a single action—while the precise number of total breach victims is unknown, on information and belief, the Data Breach has impacted

at least thousands of former and current patients;

b. **Ascertainability**. Class members are readily identifiable from information in Defendants' possession, custody, and control;

c. **Typicality**. Plaintiff's claims are typical of Class member's claims as each arises from the same Data Breach, the same alleged violations by Defendants, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. Her interests do not conflict with Class members' interests, and they have retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiff's and the Class's claims raise predominantly common factual and legal questions that a class wide proceeding can answer for all Class members. Indeed, it will be necessary to answer the following questions:

i. Whether Defendants had a duty to use reasonable care in safeguarding Plaintiff and the Class's PII and PHI;

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

iii. Whether Defendants failed to properly notify Plaintiff and the Class of the Data Breach;

iv. If Defendants were negligent in maintaining, protecting, and securing PII and PHI;

v. If Defendants took reasonable measures to determine the

extent of the Data Breach;

vi. If the Data Breach injured Plaintiff and the Class;

vii. What the proper damages measure is; and

viii. If Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

94. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiff are insufficient to make individual lawsuits economically feasible.

VI. CAUSES OF ACTION

COUNT I,
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

95. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

96. Defendants owed to Plaintiff and other members of the Class a duty to exercise reasonable care in handling and using the PII and PHI in their care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach and unauthorized transmittal and use that happened, and to promptly detect attempts at unauthorized access.

97. Defendants owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendants' failure to adequately safeguard their PII and PHI in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII and PHI—just like the Data Breach that ultimately happened. Defendants acted with wanton and reckless disregard for the security and confidentiality of

Plaintiff's and members of the Class's PII and PHI by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

98. Defendants owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII and PHI. Defendants also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and members of the Class to take appropriate measures to protect their PII and PHI, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

99. Defendants owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendants knew or should have known would suffer injury-in-fact from Defendants' inadequate website privacy protocols. Defendants actively sought and obtained Plaintiff and members of the Class's personal information and PII and PHI.

100. The risk that Defendants was transmitting sensitive PII and PHI to unauthorized third parties—namely, Facebook— was foreseeable.

101. PII and PHI is highly valuable, and Defendants knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII and PHI of Plaintiff and members of the Class's and the importance of exercising reasonable care in handling it.

102. Defendants breached their duties by failing to exercise reasonable care in supervising their agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII and PHI of Plaintiff and members of the Class which actually and proximately caused the Data Breach and Plaintiff and members of the Class's injury.

103. Defendants further breached their duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff and members of the Class's injuries-in-fact. As a direct and traceable result of Defendants' negligence and/or negligent supervision, Plaintiff and members of the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

104. Defendants' breach of their common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the unauthorized access of their PII and PHI by third parties, improper disclosure of their PII and PHI, lost benefit of their bargain, lost value of their PII and PHI, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendants' negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

105. Pursuant to CR. 8.01, the amount in controversy exceeds the minimum jurisdiction of the Jefferson Circuit Court.

COUNT II,
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

106. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

107. Under the FTC Act, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff and members of the Class's PII and PHI.

108. Section 5 of the FTC Act prohibits "unfair…practices in or affecting commerce,"

including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect customers or, in this case, patients' PII and PHI. The FTC publications and orders promulgated under the FTC Act also form part of the basis of Defendants' duty to protect Plaintiff and the members of the Class's sensitive PII and PHI.

109. Defendants violated their duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and not complying with applicable industry standards as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII and PHI Defendants had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result in the event of a breach, which ultimately came to pass.

110. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

111. Defendants had a duty to Plaintiff and the members of the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiff and the Class's PII and PHI.

112. Defendants breached its respective duties to Plaintiff and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and members of the Class's PII and PHI.

113. Defendants' violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence per se.

114. But for Defendants' wrongful and negligent breach of its duties owed to

Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

115. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that Defendants was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII and PHI.

116. On information and belief, Defendants are each a covered entity and/or business associate under the HIPAA (42 U.S.C. § 1302d, *et seq*.). As an entity covered by HIPAA, Defendants had a duty to implement reasonable safeguards to protect Plaintiff's and Class members' PHI.

117. Under HIPAA, Defendants had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 C.F.R. § 164.304 definition of encryption).

118. Plaintiff and Class members are within the class of persons that the HIPAA was intended to protect.

119. The harm that occurred as a result of the Data Breach is the type of harm that HIPAA was intended to guard against. The Federal Health and Human Services' Office for Civil Rights ("OCR") has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures relating to protected health information, caused the same harm as that suffered by Plaintiff and the Class members.

120. Defendants breached their duties to Plaintiff and the Class under HIPAA, by failing to provide fair, reasonable, or adequate computer systems and data security practices

to safeguard Plaintiff's and Class members' PHI.

121. Defendants' failure to comply with applicable laws and regulations, including the FTC Act, constitutes negligence *per se*.

122. But for Defendants' wrongful and negligent breach of its duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

123. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that Defendants was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PHI.

124. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and members of the Class have suffered harm, including; lost control over the value of PII and PHI; and other harm resulting from the unauthorized use or threat of unauthorized use of collected personal information, entitling them to damages in an amount to be proven at trial.

125. Pursuant to CR. 8.01, the amount in controversy exceeds the minimum jurisdiction of the Jefferson Circuit Court.

COUNT III,
INVASION OF PRIVACY, INTRUSION UPON SECLUSION
(On Behalf of Plaintiff and the Class)

126. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

127. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and PHI and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

128. Defendants owed a duty to their patients, including Plaintiff and the Class, to

keep this information confidential.

129. The unauthorized acquisition by a third party of Plaintiff's and Class Members' PII and PHI from Defendants is highly offensive to a reasonable person.

130. The intrusion was into a place or thing which was private and entitled to be private.

131. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

132. The Data Breach constitutes an intentional interference with Plaintiff's and the Class's 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.

133. Defendants acted with a knowing and intentional state of mind when they permitted the Data Breach because they knew its information security practices were inadequate.

134. Defendants acted with a knowing and intentional state of mind when they failed to notify Plaintiff and the Class about the Data Breach, thereby materially impairing their mitigation efforts.

135. Acting with knowledge, Defendants had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

136. As a direct and proximate result of Defendants' acts and omissions, the private and sensitive PII and PHI of Plaintiff and the Class were transmitted to and accessed by an unauthorized third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

137. Unless and until enjoined and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII and PHI are still maintained by Defendants with their inadequate website

privacy system and policies.

138. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendants' continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendants' inability to safeguard the PII and PHI of Plaintiff and the Class.

139. In addition to injunctive relief, Plaintiff, on behalf of herself, C.S., and the other members of the Class, also seeks compensatory damages for Defendants' invasion of privacy, which includes the value of the privacy interest invaded by Defendants, the costs of future monitoring of their personal information, plus prejudgment interest, and costs.

140. Pursuant to CR. 8.01, the amount in controversy exceeds the minimum jurisdiction of the Jefferson Circuit Court.

COUNT IV,
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

141. Plaintiff and members of the Class incorporate all previous paragraphs as if fully set forth herein.

142. Defendants offered health services to Plaintiff, C.S., and members of the Class. Then, Plaintiff and members of the Class accepted Defendants' services—and paid for those services. And when Plaintiff and members of the Class paid for the services, they also provided their PII and PHI to Defendants.

143. Thus, Plaintiff and members of the Class entered implied contracts with Defendants. And so, each purchase before and during the Data Breach was made under these mutually agreed-upon implied contracts with Defendants.

144. Under those implied contracts, Defendants agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and members of the Class if their information was compromised and or accessed without authorization.

145. After all, Plaintiff and the members of the Class would not have provided and entrusted their PII and PHI to Defendants in the absence of an implied contract.

146. Defendants materially breached the contracts they entered with Plaintiff and members of the Class by:

a. Transmitting the PII and PHI of Plaintiff and the Class to third-parties without authorization;

b. Failing to safeguard and protect the PII and PHI of Plaintiff and the members of the Class;

c. Failing to promptly notify Plaintiff and members of the Class of the Data Breach— and the subsequent exposure and unauthorized access of their PII and PHI;

d. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and,

e. Failing to ensure the confidentiality and integrity of the electronic PII and PHI that Defendants created, maintained, received, and transmitted.

147. The damages sustained by Plaintiff and members of the Class as described above were the direct and proximate result of Defendants' material breaches of its agreements.

148. Plaintiffs and members of the Class performed as required under the relevant agreement—or such performance was waived by the conduct of Defendants.

149. All contracts include the covenant of good faith and fair dealing—thus, all contracts impose on each party a duty of good faith and fair dealing. As a result:

a. The parties must act with honesty in fact in the conduct or transactions concerned;

b. The parties must act with good faith and fair dealing when executing contracts and discharging performance and other duties according to their terms—as to preserve the spirit, and not merely the letter, of the bargain; and,

c. The parties are mutually obligated to comply with both the substance and form of their contracts.

150. Subterfuge and evasion violate the duty of good faith in performance—even when an actor believes their conduct is justified. Bad faith may be overt or may consist of inaction. And fair dealing may require more than honesty.

151. Here, Defendants failed to advise Plaintiff and members of the Class of the Data Breach promptly and sufficiently. In these and other ways, Defendants violated its duty of good faith and fair dealing.

152. Simply put, Defendants—through its numerous material breaches of the implied contracts—injured both Plaintiff and the members of the Class.

153. Pursuant to CR. 8.01, the amount in controversy exceeds the minimum jurisdiction of the Jefferson Circuit Court.

COUNT V,
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

154. Plaintiff and members of the Class incorporate all previous paragraphs as if fully set forth herein.

155. This claim is pled in the alternative to the claim of breach of implied contract.

156. Plaintiff and members of the Class conferred benefits upon Defendants in the

form of payments for health services. Also, Defendants received additional benefits from receiving the PII and PHI of Plaintiff and members of the Class—such data is used to facilitate both payment and the provision of services.

157. Defendants appreciated or knew of these benefits that it received. And under principles of equity and good conscience, this court should not allow Defendants to retain the full value of these benefits—specifically, the payments, PII, and PHI of Plaintiff and members of the Class.

158. After all, Defendants failed to adequately protect their PII and PHI. And if such inadequacies were known, then Plaintiff and the members of the class would never have conferred payment nor disclosed their PII and PHI.

159. Defendants should be compelled to disgorge into a common fund—for the benefit of Plaintiff and members of the Class—all funds that were unlawfully or inequitably gained despite Defendants' misconduct and the resulting Data Breach.

160. Pursuant to CR. 8.01, the amount in controversy exceeds the minimum jurisdiction of the Jefferson Circuit Court.

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

161. Plaintiff and members of the Class incorporate all previous paragraphs as if fully set forth herein.

162. In providing their private information to Defendants, Plaintiff and Class Members justifiably placed special confidence in Defendants to act in good faith and with due regard to the interests of Plaintiff and Class Members in order to safeguard and keep confidential that PII and PHI.

163. Defendants accepted the special confidence placed in it by Plaintiff and Class Members, as evidenced by its assertion in its Notice of Privacy Practices that it "will not use

or share your information other than as described here unless you tell us we can in writing," and by the promulgation of this privacy policy and Online Privacy Practices. There was an understanding between the parties that Defendants would act for the benefit of Plaintiff and Class Members in preserving the confidentiality of this PII and PHI.

164. In light of the special relationship between Defendants, Plaintiff, C.S., and the Class Members, whereby Defendant became the guardian of Plaintiff's and the Class Members' private information, Defendant accepted a fiduciary duty to act primarily for the benefit of its patients, including Plaintiff and the Class Members. This duty included safeguarding Plaintiff's and the Class Members' private information.

165. Defendants have a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of its medical relationship with its patients, in particular, to keep secure the Private Information of those patients.

166. Defendants breached their fiduciary duties to Plaintiff and Class Members by failing to diligently discover, investigate, or give notice of the Data Breach in a reasonable and practicable period of time.

167. Defendants breached their fiduciary duties to Plaintiff and the Class Members by transmitting their PII and PHI to third-parties via the Meta Pixel.

168. Defendants breached the fiduciary duties it owed to Plaintiff and the Class Members by failing to timely notify and/or warn them of the Data Breach

169. Defendants breached their fiduciary duties by failing to ensure the confidentiality and integrity of electronic PHI Defendants created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1).

170. Defendants breached their fiduciary duties by failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R.

§ 164.306(a)(3).

171. Defendants breached their fiduciary duties by failing to ensure compliance with the HIPAA security standard rules by its workforce, in violation of 45 C.F.R. § 164.306(a)(94).

172. Defendants breached their fiduciary duties by impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons, in violation of 45 C.F.R. § 164.502, *et seq*.

173. Defendant breached their fiduciary duties by failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures necessary to maintain the security of PHI, in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5).

174. Defendants breached their fiduciary duties by failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in violation of 45 C.F.R. § 164.530(c).

175. Defendants breached their fiduciary duties by otherwise failing to safeguard Plaintiff's and the Class Members' private information.

176. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, as set forth above.

177. As a direct and proximate result of Defendants' breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

178. Pursuant to CR 8.01, the amount in controversy exceeds the minimum jurisdiction of the Jefferson Circuit Court.

COUNT VII,
VIOLATION OF THE KENTUCKY CONSUMER PROTECTION ACT,
KRS § 367.110, *ET SEQ.*
(On Behalf of Plaintiff and the Class)

179. Plaintiff and members of the Class incorporate all previous paragraphs as if fully set forth herein.

180. The Kentucky Consumer Protection Act, KRS § 367.110, *et seq.,* prohibits any "unfair, false, misleading, or deceptive acts or practices in the conduct of any trade or commerce." KRS § 367.170.

181. Defendants are each a "person" as defined by KRS § 367.110.

182. By conduct set forth in the preceding paragraphs, Defendants engaged in the complained-of conduct in connection with "trade" and "commerce" with regard to "services" as defined by KRS § 367.110. Defendants advertised, offered, or sold services relating to the medical treatment of Plaintiffs and Class Members.

183. Defendants engaged in deceptive acts and practices by using deception, fraud, false pretense, false promise, and misrepresentation in connection with trade and commerce, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' PII and PHI, which was a direct and proximate cause of the Data Breach;

b. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' PII and PHI, which was a direct and proximate cause of the Data Breach;

c. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class Members' PII and PHI, including by not disclosing PII and PHI for marketing purposes without proper authorization;

d. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' PII and PHI; and

e. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII and PHI.

184. Defendants intended to mislead Plaintiff and Class members and induce them to rely on their misrepresentations and omissions in order to provide medical treatment to Plaintiffs and Class Members, and in order to receive their valuable PII and PHI.

185. Defendants' representations and omissions, made at the time of the relevant transactions, were material because they were likely to deceive reasonable consumers, including Plaintiff and Class Members, about the security of the PII and PHI entrusted to Defendants.

186. Had Defendants disclosed to Plaintiffs and Class Members that its data systems were not secure and that their PII and PHI would be disclosed to third-parties, including Facebook via the Metal Pixel without authorization, Defendants would have been unable to continue in business and would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiff's and Class Members' PII and PHI as part of the medical services relationship between Defendants and Plaintiff and Class Members without advising Plaintiff and Class Members that Defendant's data security practices were insufficient to maintain the safety and confidentiality of Plaintiff's and Class Members' information. Accordingly, Plaintiff and the Class Members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

187. Defendants had a duty to disclose these facts due to the circumstances of this case and the sensitivity and extensivity of the information in its possession. In addition, such

a duty is implied by law due to the nature of the relationship between medical patients—including Plaintiff, C.S., and the Class—and Defendants, because medical patients are unable to fully protect their interests with regard to their data, and placed trust and confidence in Defendants. Defendants' duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems, and that they were transmitting PII and PHI to third-parties for marketing purposes;

b. Active concealment of the state of its security and disclosures; and,

c. Incomplete representations about the security and integrity of its computer and data systems while purposefully withholding material facts from Plaintiff and the Class that contradicted these representations.

188. Defendants acted intentionally, knowingly, and maliciously to violate Kentucky's Consumer Protection Act, and recklessly disregarded Plaintiff's and Class Members' rights. Defendant was on notice that its security and privacy protections were inadequate and resulted in transmission of PII and PHI without authorization. An award of punitive damages would serve to punish Defendants for their wrongdoing and warn or deter others from engaging in similar conduct.

189. As a direct and proximate result of Defendants' deceptive acts or practices, Plaintiff and Class Members have suffered and will continue to suffer injury, and damages as set forth herein, including loss of the benefit of their bargain with Defendants as they would not have sought medical services from Defendants but for Defendants' violations alleged herein; diminution and loss of value of their private information; and an increased, imminent risk of fraud and identity theft.

190. Defendants' violations present a continuing risk to Plaintiff and Class Members as well as to the general public.

191. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including actual damages, restitution, injunctive relief, punitive damages, and attorneys' fees and costs.

192. Pursuant to CR 8.01, the amount in controversy exceeds the minimum jurisdiction of the Jefferson Circuit Court.

COUNT VIII,
VIOLATION OF KRS § 365.732,
NOTIFICATION TO AFFECTED PERSONS OF COMPUTER SECURITY BREACH INVOLVING THEIR UNENCRYPTED PERSONALLY IDENTIFIABLE INFORMATION
(On Behalf of Plaintiff and the Class)

193. Plaintiff and members of the Class incorporate all previous paragraphs as if fully set forth herein.

194. KRS § 365.732 ("Notification to affected persons of computer security breach involving their unencrypted personally identifiable information") at KRS § 365.732(1)(a), defines a "Breach of the security of the system" as an:

> unauthorized acquisition of unencrypted and unredacted computerized data that compromises the security, confidentiality, or integrity of personally identifiable information maintained by the information holder as part of a database regarding multiple individuals that actually causes, or leads the information holder to reasonably believe has caused or will cause, identity theft or fraud against any resident of the Commonwealth of Kentucky. Good-faith acquisition of personally identifiable information by an employee or agent of the information holder for the purposes of the information holder is not a breach of the security of the system if the personally identifiable information is not used or subject to further unauthorized disclosure.

195. At all relevant times, Defendants were each an "information holder," as defined by KRS § 365.732(1)(b) as each are a "…business entity that conducts business in this state."

196. KRS § 365.732(1)(c) further defines "Personally identifiable information" as "an individual's first name or first initial and last name in combination with any one (1) or more of the following data elements, when the name or data element is not redacted: 1. Social Security number…".

197. As set forth above, Defendants had possession of the Personally Identifiable Information (PII), of Plaintiff and the proposed Class, via the Meta Pixel.

198. Defendants' disclosure of the PII and/or PHI of Plaintiff and the proposed Class members to Facebook via the Meta Pixel, the Data Breach, constitutes a "breach of the security of the system" as defined by KRS § 365.731(1)(a).

199. KRS § 365.732(2) provides that:

> [a]ny information holder **shall disclose any breach of the security of the system**, following discovery or notification of the breach in the security of the data, to any resident of Kentucky whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. **The disclosure shall be made in the most expedient time possible and without unreasonable delay**…

KRS § 365.732(2) (emphases added).

200. Defendants have failed to disclose the Data Breach to Plaintiff and the proposed Class members in accordance with KRS § 365.732(2).

201. As a direct and/or proximate result of the Defendants' failure to notify the Plaintiff and Class members of the breach, they were caused, or will be imminently caused, injury and damages as set forth herein, including loss of the opportunity to control how their PII and PHI is used; diminution in value of their PII and PHI; compromise and continuing publication of their PII and PHI; and, identity theft and fraudulent charges.

202. Pursuant to CR 8.01, the amount in controversy exceeds the minimum jurisdiction of the Jefferson Circuit Court.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, RHONDA BLANDFORD, Individually, and as Mother and Next Friend of C.S., on behalf of herself, and all others similarly situated, the proposed Class Members, demand judgment against the Defendants, UOFL HEALTH, INC., and UNIVERSITY OF LOUISVILLE PHYSICIANS, INC. d/b/a UOFL PHYSICIANS, in the

manner as follows:

A. Trial by jury;

B. An Order certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing her counsel to represent the Class;

C. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

D. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

E. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

F. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

G. Enjoining Defendants from further deceptive practices and making untrue statements about the Data Breach and the transmitted PII and PHI;

H. Awarding attorneys' fees and costs, as allowed by law;

I. Awarding prejudgment and post-judgment interest, as provided by law;

J. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and,

K. Any and all such other relief to which Plaintiff and the Class are entitled.

Dated: March 21, 2023

Respectfully submitted,

/s/ Andrew E. Mize

J. Gerard Stranch, IV (*Pro Hac Vice* forthcoming)
Andrew E. Mize (Ky. Bar No. 94453)
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200

Nashville, Tennessee 37203
(615) 254-8801
(615) 255-5419 (facsimile)
Gstranch@stranchlaw.com
amize@stranchlaw.com

Lynn A. Toops (*Pro Hac Vice* forthcoming)
Amina A. Thomas (*Pro Hac Vice* forthcoming)
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
ltoops@cohenandmalad.com
athomas@cohenandmalad.com

Samuel J. Strauss (*Pro Hac Vice* forthcoming)
TURKE & STRAUSS, LLP
613 Williamson St., Suite 201
Madison, Wisconsin 53703
(608) 237-1775
(608) 509-4423 (facsimile)
sam@turkestrauss.com
raina@turkestrauss.com

Counsel for Plaintiff and the Proposed Class