IN THE SUPERIOR COURT FOR THE STATE OF WASHINGTON
IN AND FOR KING COUNTY

NICOLE WHITCRAFT, individually, and on behalf of all others similarly situated, Plaintiff, v. CELLNETIX LABS, LLC and CELLNETIX PATHOLOGY, PLLC, Defendants.	NO. CLASS ACTION COMPLAINT

Plaintiff Nicole Whitcraft ("Plaintiff"), individually, and on behalf of all others similarly situated, brings this action against the CellNetix Labs, LLC and CellNetix Pathology, PLLC (collectively "CellNetix" or "Defendants"). Plaintiff brings this action by and through her attorneys, and alleges, based upon personal knowledge as to her own actions, and based upon information and belief and reasonable investigation by her counsel as to all other matters, as follows.

I. INTRODUCTION

1. Defendants provide lab testing and diagnostics services to patients throughout the Pacific Northwest.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

2. As part of its operations, Defendants collect, maintain, and store highly sensitive personal and medical information belonging to their patients and employees, including, but not limited to, their full names, Social Security numbers, dates of birth, driver's license numbers, passport numbers ("personally identifying information" or "PII"), and health insurance policy and health insurance identification numbers (collectively "Private Information").

3. On December 10, 2023, unauthorized cybercriminals accessed Defendants' information systems and databases and stole Private Information belonging to Defendants' current and former patients and employees, including Plaintiff and Class members (the "Data Breach"). On December 19, 2023, Defendants determined that Private Information concerning their patients and employees was compromised in the Data Breach, including their full names, Social Security numbers, driver's license or state ID numbers, dates of birth, military identification numbers, passport numbers, health insurance policy numbers, and health insurance identification numbers.

4. Because Defendants stored and handled the highly-sensitive Private Information, they had a duty and obligation to safeguard this information and prevent unauthorized third parties from accessing this data.

5. Defendants failed to fulfill this obligation, as unauthorized cybercriminals breached Defendants' information systems and databases and stole vast quantities of Private Information belonging to their patients, including Plaintiff and Class members. This breach--and the successful exfiltration of Private Information—were direct, proximate, and foreseeable results of multiple failings on the part of Defendants.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

6. The data breach occurred because Defendants failed to implement reasonable security protections to safeguard their information systems and databases. Further, Defendants failed to inform the public that their data security practices were deficient and inadequate.

7. As a result of Defendants' negligent, reckless, intentional, and/or unconscionable failure to adequately satisfy their contractual, statutory, and common-law obligations, Plaintiff and Class members suffered injuries including, but not limited to:

- Lost or diminished value of their Private Information;
- Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information;
- Lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges;
- Time needed to investigate, correct and resolve unauthorized access to their accounts; time needed to deal with spam messages and e-mails received subsequent to the Data Breach;
- Charges and fees associated with fraudulent charges on their accounts; and
- The continued and increased risk of compromise to their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect their Private Information.

8. Accordingly, Plaintiff brings this action on behalf of all those similarly situated to seek relief for the consequences of Defendants' failure to reasonably safeguard Plaintiff's and Class members' Private Information.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

II. PARTIES

Plaintiff Nicole Whitcraft

9. Plaintiff Whitcraft is a resident and citizen of Federal Way, Washington. Plaintiff Whitcraft was employed by CellNetix. Plaintiff Whitcraft received Defendants' Data Breach Notice.

Defendant CellNetix Labs, LLC

10. Defendant CellNetix Labs, LLC is a Washington limited liability corporation with its principal place of business located at 12501 E Marginal Way S, Ste. 200, Tukwila, WA, 98168-5163. It provides medical diagnosis and laboratory testing services throughout the Pacific Northwest under the business name CellNetix Pathology and Laboratories.

CellNetix Pathology, PLLC

11. Defendant CellNetix Pathology, PLLC is a Washington professional limited liability corporation with its principal place of business located at 12501 E Marginal Way S, Ste. 200, Tukwila, WA, 98168-5163. It provides medical diagnosis and laboratory testing services throughout the Pacific Northwest under the business name CellNetix Pathology and Laboratories.

III. JURISDICTION AND VENUE

12. This Court has jurisdiction over Proliance because Proliance is a resident and citizen of the State of Washington, and its headquarters is in King County.

13. Venue is proper in this County under RCW 4.12.025 because a substantial part of the events or omissions giving rise to Plaintiff's and Class members' claims occurred in this County and because Defendant resides in this County.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

IV. FACTUAL ALLEGATIONS

A. CellNetix Pathology and Laboratories – Background

14. CellNetix Pathology and Laboratories provides a variety of screening, diagnoses, and laboratory testing services to patients throughout the Pacific Northwest. It primarily serves hospitals and other healthcare providers and offers a wide range of pathology services, including molecular pathology, pediatric pathology, cytopathology, and liver pathology. As part of its operations, it collects, maintains, and stores the highly sensitive PII and medical information provided by its current and former patients, including but not limited to their full names, Social Security numbers, dates of birth, health insurance information, driver's license numbers, and passport information.

15. On information and belief, Defendants CellNetix Labs and CellNetix Pathology operate a joint venture under the name CellNetix Pathology and Laboratories.

16. Defendants failed to implement necessary data security safeguards at the time of the Data Breach. This failure resulted in cybercriminals accessing the Private Information of their current and former patients and employees—Plaintiff and Class members.

17. Defendants' current and former patients and employees, such as Plaintiff and Class members, made their Private Information available to Defendants with the reasonable expectation that any entity with access to this information would keep that sensitive and personal information confidential and secure from illegal and unauthorized access. They similarly expected that, in the event of any unauthorized access, these entities would provide them with prompt and accurate notice.

18. This expectation was objectively reasonable and based on an obligation imposed on Defendants by statute, regulations, industrial custom, and standards of general due care.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

19. Unfortunately for Plaintiff and Class members, Defendants failed to carry out their duty to safeguard sensitive Private Information and provide adequate data security. As a result, they failed to protect Plaintiff and Class members from having their Private Information accessed and stolen during the Data Breach.

B. The Data Breach

20. According to Defendants' public statements, cybercriminals breached Defendants' information systems and databases on or before December 10, 2023.

21. On or about December 19, 2023, Defendants determined that the following categories of information had been compromised in the Data Breach: full names, Social Security numbers, driver's license numbers, state ID numbers, dates of birth, military ID numbers, passport ID numbers, health insurance policy numbers, and health insurance ID numbers.

22. On January 8, 2024, Defendants sent out a data breach notice to all individuals whose Private Information was compromised in the Data Breach.

C. Defendants' Many Failures Both Prior to and Following the Data Breach

23. Defendants collect and maintain vast quantities of Private Information belonging to Plaintiff and Class members as part of its normal operations as a healthcare service provider. The Data Breach occurred as direct, proximate, and foreseeable results of multiple failings on the part of Defendants.

24. First, Defendants failed to implement reasonable security protections to safeguard their information systems and databases.

25. Second, Defendants failed to inform the public that their data security practices were deficient and inadequate. Had Plaintiff and Class members been aware that Defendants

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

did not have adequate safeguards in place to protect such sensitive Private Information, they would have never provided such information to Defendants.

26. Defendants' attempt to ameliorate the effects of this data breach with 1 year of complimentary credit monitoring is inadequate. Plaintiff's and Class members' Private Information was accessed and acquired by cybercriminals for the express purpose of misusing the data. As a consequence, they face the real, immediate, and likely danger of identity theft and misuse of their Private Information. And this can, and in some circumstances already has, caused irreparable harm to their personal, financial, reputational, and future well-being. This harm is even more acute because much of the stolen Private Information is immutable.

D. Data Breaches Pose Significant Threats

27. Data breaches have become a constant threat that, without adequate safeguards, can expose personal data to malicious actors. It is well known that PII, and Social Security numbers in particular, is an invaluable commodity and a frequent target of hackers.

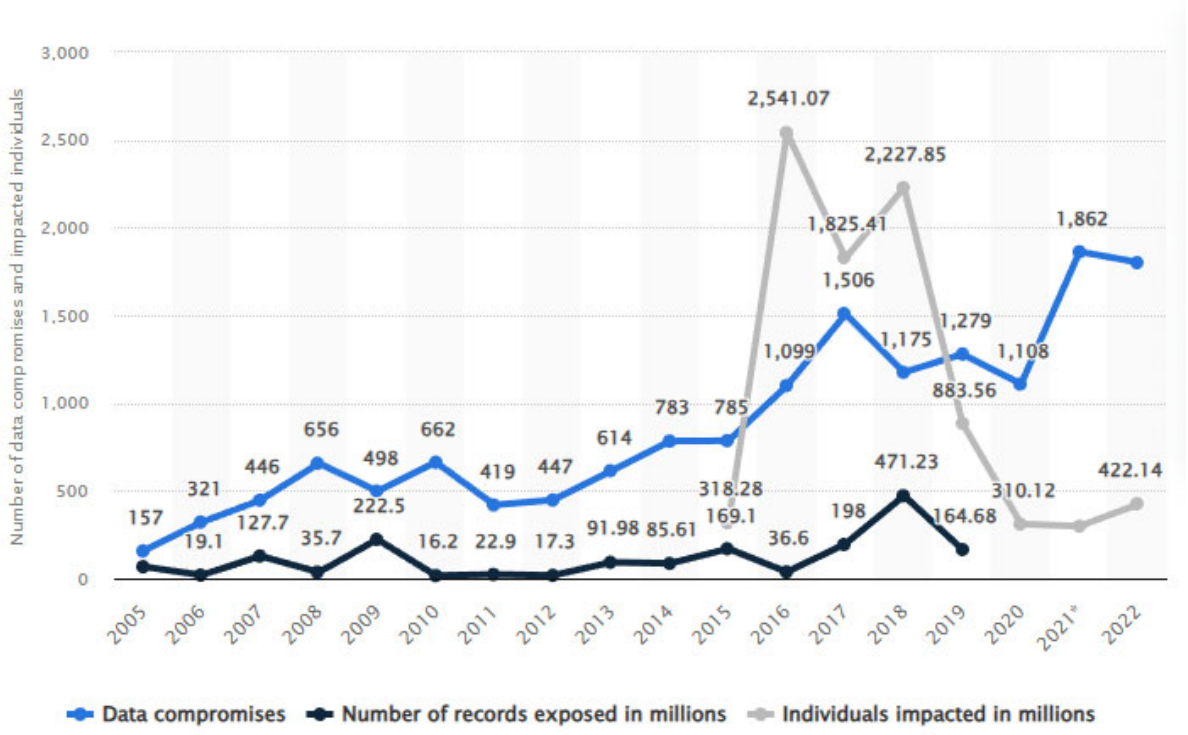
28. In 2022, the Identity Theft Resource Center's Annual End-of-Year Data Breach Report listed 1,802 total compromises involving 422,143,312 victims for 2022, which was just 50 compromises short of the current record set in 2021.[1] The HIPAA Journal's 2022 Healthcare Data Breach Report reported 707 compromises involving healthcare data, which is just 8 shy of the record of 715 set in 2021 and still double that of the number of similar such compromises in 2017 and triple the number of compromises in 2012.[2]

[1] *2022 End of Year Data Breach Report*, Identity Theft Resource Center (January 25, 2023), available at: https://www.idtheftcenter.org/publication/2022-data-breach-report/?utm_source=press+release&utm_medium=web&utm_campaign=2022+Data+Breach+Report+.

[2] *2022 Healthcare Data Breach Report*, The HIPAA Journal (January 24, 2023), available at: https://www.hipaajournal.com/2022-healthcare-data-breach-report/.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

29. Statista, a German entity that collects and markets data relating to, among other things, data breach incidents and the consequences thereof, confirms that the number of data breaches has been steadily increasing since it began a survey of data compromises in 2005 with 157 compromises reported that year, to a peak of 1,862 in 2021, to 2022's total of 1,802.[3] The number of impacted individuals has also risen precipitously from approximately 318 million in 2015 to 422 million in 2022, which is an increase of nearly 50%.[4]



[3] *Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2022*, Statista, available at: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.

[4] *Id.*

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

30. This stolen PII is then routinely traded on dark web black markets as a simple commodity, with Social Security numbers being so ubiquitous to be sold at as little as $2.99 apiece and passports retailing for as little as $15 apiece.[5]

31. In addition, the severity of the consequences of a compromised Social Security number belies the ubiquity of stolen numbers on the dark web. Criminals and other outfits can fraudulently take out loans under the victims' name, open new lines of credit, and cause other serious financial difficulties for victims:

> [a] dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[6]

This is exacerbated by the fact that the problems arising from a compromised Social Security number are exceedingly difficult to resolve. A victim is forbidden from proactively changing his or her number unless and until it is actually misused and harm has already occurred. And even this delayed remedial action is unlikely to undo the damage already done to the victims:

> Keep in mind that a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.[7]

---

[5] *What is your identity worth on the dark web?* Cybernews (September 28, 2021), available at: https://cybernews.com/security/whats-your-identity-worth-on-dark-web/.

[6] United States Social Security Administration, *Identity Theft and Your Social Security Number*, United States Social Security Administration (July 2021), available at: https://www.ssa.gov/pubs/EN-05-10064.pdf.

[7] *Id.*

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

32. The most sought after and expensive information on the dark web are stolen medical records which command prices from $250 to $1,000 each.[8] Medical records are considered the most valuable because unlike credit cards, which can easily be canceled, and Social Security numbers, which can be changed, medical records contain "a treasure trove of unalterable data points, such as a patient's medical and behavioral health history and demographics, as well as their health insurance and contact information."[9] With this bounty of ill-gotten information, cybercriminals can steal victims' public and insurance benefits and bill medical charges to victims' accounts.[10] Cybercriminals can also change the victims' medical records, which can lead to misdiagnosis or mistreatment when the victims seek medical treatment.[11] Victims of medical identity theft could even face prosecution for drug offenses when cybercriminals use their stolen information to purchase prescriptions for sale in the drug trade.[12]

33. The wrongful use of compromised medical information is known as medical identity theft and the damage resulting from medical identity theft is routinely far more serious than the harm resulting from the theft of simple PII. Victims of medical identity theft spend an average of $13,500 to resolve problems arising from medical identity theft and there are

---

[8] Paul Nadrag, Capsule Technologies, *Industry Voices—Forget credit card numbers. Medical records are the hottest items on the dark web*, Fierce Healthcare (January 26, 2021), available at: https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web.

[9] *Id.*

[10] *Medical Identity Theft in the New Age of Virtual Healthcare*, IDX (March 15, 2021), available at https://www.idx.us/knowledge-center/medical-identity-theft-in-the-new-age-of-virtual-healthcare. *See also* Michelle Andrews, *The Rise of Medical Identity Theft*, Consumer Reports (August 25, 2016), available at https://www.consumerreports.org/health/medical-identity-theft-a1699327549/.

[11] *Id.*

[12] *Id.*

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

currently no laws limiting a consumer's liability for fraudulent medical debt (in contrast, a consumer's liability for fraudulent credit card charges is capped at $50).[13] It is also "considerably harder" to reverse the damage from the aforementioned consequences of medical identity theft.[14]

34. Instances of Medical identity theft have grown exponentially over the years from approximately 6,800 cases in 2017 to just shy of 43,000 in 2021, which represents a seven-fold increase in the crime.[15]

35. In light of the dozens of high-profile health and medical information data breaches that have been reported in recent years, entities like Defendants charged with maintaining and securing patient PII should know the importance of protecting that information from unauthorized disclosure. Indeed, Defendants knew, or certainly should have known, of the recent and high-profile data breaches in the health care industry: UnityPoint Health, Lifetime Healthcare, Inc., Community Health Systems, Kalispell Regional Healthcare, Anthem, Premera Blue Cross, and many others.[16]

36. In addition, the Federal Trade Commission ("FTC") has brought dozens of cases against companies that have engaged in unfair or deceptive practices involving inadequate protection of consumers' personal data, including recent cases concerning health-related information against LabMD, Inc., SkyMed International, Inc., and others. The FTC publicized

[13] Medical Identity Theft, AARP (March 25, 2022), available at: https://www.aarp.org/money/scams-fraud/info-2019/medical-identity-theft.html.

[14] *Id.*

[15] *Id.*

[16] *See, e.g.*, *Healthcare Data Breach Statistics*, HIPAA Journal, available at: https://www.hipaajournal.com/healthcare-data-breach-statistics.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

these enforcement actions to place companies like Defendants on notice of their obligation to safeguard customer and patient information.[17]

37. Given the nature of Defendants' Data Breach, as well as the length of the time Defendants' networks were breached, it is foreseeable that the compromised Private Information has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiff's and Class members' Private Information can easily obtain Plaintiff's and Class members' tax returns or open fraudulent credit card accounts in Class members' names.

38. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because credit card victims can cancel or close credit and debit card accounts.[18] The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

39. To date, Defendants have offered its consumers a mere 12-months of identity theft monitoring services. The offered services are inadequate to protect Plaintiff and the Class from the threats they will face for years to come, particularly in light of the Private Information at issue here.

40. Despite the prevalence of public announcements of data breach and data security compromises, its own acknowledgment of the risks posed by data breaches, and its own

---

[17] *See e.g.*, *In the Matter of SKYMED INTERNATIONAL, INC.*, C-4732, 1923140 (F.T.C. Jan. 26, 2021).

[18] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, Forbes (Mar 25, 2020), available at https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1. *See also Why Your Social Security Number Isn't as Valuable as Your Login Credentials*, Identity Theft Resource Center (June 18, 2021), available at https://www.idtheftcenter.org/post/why-your-social-security-number-isnt-as-valuable-as-your-login-credentials/.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

acknowledgment of its duties to keep Private Information private and secure, Defendants failed to take appropriate steps to protect the Private Information of Plaintiff and the Class from misappropriation. As a result, the injuries to Plaintiff and the Class were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for its current and former patients and employees.

E. Defendants Had a Duty and Obligation to Protect Private Information

41. Defendants have an obligation to protect the Private Information belonging to Plaintiff and Class members. First, this obligation was mandated by government regulations and state laws, including HIPAA and FTC rules and regulations. Second, this obligation arose from industry standards regarding the handling of sensitive Private Information. Plaintiff and Class members provided, and Defendants obtained, their information on the understanding that it would be protected and safeguarded from unauthorized access or disclosure.

i. HIPAA Requirements and Violation

42. HIPAA requires, *inter alia*, that Covered Entities and Business Associates implement and maintain policies, procedures, systems and safeguards that ensure the confidentiality and integrity of consumer and patient PII and PHI, protect against any reasonably anticipated threats or hazards to the security or integrity of consumer and patient PII and PHI, regularly review access to data bases containing protected information, and implement procedures and systems to detect, contain, and correct any unauthorized access to protected information. *See* 45 CFR § 164.302, *et seq.*

43. HIPAA, as applied through federal regulations, also requires private information to be stored in a manner that renders it, "unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology. . ." 45 CFR § 164.402.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

44. Defendants failed to implement and/or maintain procedures, systems, and safeguards to protect the Private Information belonging to Plaintiff and the Class from unauthorized access and disclosure.

45. Upon information and belief, Defendants' security failures include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information Defendants create, receive, maintain, and transmit in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents;

g. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii);

h. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2);

i. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3);

j. Failing to ensure compliance with HIPAA security standard rules by Defendants' workforce, in violation of 45 CFR 164.306(a)(94); and

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

46. Upon information and belief, Defendants also failed to store the information it collected in a manner that rendered it, "unusable, unreadable, or indecipherable to unauthorized persons," in violation of 45 CFR § 164.402.

47. Because Defendants have failed to comply with HIPAA, while monetary relief may cure some of Plaintiff's and Class members' injuries, injunctive relief is also necessary to ensure Defendants' approach to information security is adequate and appropriate going forward. Defendants still maintain the highly sensitive Private Information of its current and former patients and employees, including Plaintiff and Class members. Without the supervision of the Court through injunctive relief, Plaintiff's and Class members' Private Information remains at risk of subsequent data breaches.

ii. FTC Act Requirements and Violations

48. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

49. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

practices for business.[19] The guidelines note businesses should protect the personal 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 security problems.[20] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[21] Defendants clearly failed to do any of the foregoing, as evidenced by the length of the Data Breach, the fact that the Data Breach went undetected, and the amount of data exfiltrated.

50. 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 the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

51. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data

---

[19] *Protecting Personal Information: A Guide for Business*, Federal Trade Comm'n (October 2016), available at https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.

[20] *Id.*

[21] *Id.*

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

52. Additionally, the FTC Health Breach Notification Rule obligates companies that suffered a data breach to provide notice to every individual affected by the data breach, as well as notifying the media and the FTC. *See* 16 CFR 318.1, *et seq.*

53. As evidenced by the Data Breach, Defendants failed to properly implement basic data security practices. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

54. Defendants were fully aware of their obligation to protect the Private Information of their current and former patients, including Plaintiff and the Class. Defendants are sophisticated and technologically-savvy health care services providers that rely extensively on technology systems and networks to maintain their practice, including storing their patients' and employees' PII, protected health information, and medical information in order to operate their business.

55. Defendants had and continue to have a duty to exercise reasonable care in collecting, storing, and protecting the Private Information from the foreseeable risk of a data breach. The duty arises out of the special relationship that exists between Defendants and Plaintiff and Class members. Defendants alone had the exclusive ability to implement adequate security measures to its cyber security network to secure and protect Plaintiff's and Class members' Private Information.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

iii. Industry Standards and Noncompliance

56. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

57. Some industry best practices that should be implemented by businesses dealing with sensitive Private Information like Defendants include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendants failed to follow some or all of these industry best practices.

58. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendants failed to follow these cybersecurity best practices.

59. Defendants should have also followed the minimum standards of any one of 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 in reasonable cybersecurity readiness.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

60. Defendants failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

F. Plaintiff and the Class Suffered Harm Resulting from the Data Breach

61. Like any data hack, the Data Breach presents major problems for all affected.[22]

62. The FTC warns the public to pay particular attention to how they keep personally identifying information including Social Security numbers and other sensitive data. As the FTC notes, "once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[23]

63. The ramifications of Defendants' failure to properly secure Plaintiff's and Class members' Private Information are severe. Identity theft occurs when someone uses another person's financial, and personal information, such as that person's name, address, Social Security number, and other information, without permission in order to commit fraud or other crimes.

64. According to data security experts, one out of every four data breach notification recipients become a victim of identity fraud.

65. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for an information breach to be detected.

[22] Paige Schaffer, *Data Breaches' Impact on Consumers*, Insurance Thought Leadership (July 29, 2021), available at https://www.insurancethoughtleadership.com/cyber/data-breaches-impact-consumers.

[23] *Warning Signs of Identity Theft*, Federal Trade Comm'n, available at https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

66. Accordingly, Defendants' wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff and the Class at an imminent, immediate, and continuing increased risk of identity theft and identity fraud. According to a recent study published in the scholarly journal "Preventive Medicine Reports," public and corporate data breaches correlate to an increased risk of identity theft for victimized consumers.[24] The same study also found that identity theft is a deeply traumatic event for the victims, with more than a quarter of victims still experiencing sleep problems, anxiety, and irritation even six months after the crime.[25]

67. There is also a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that has not yet been exploited by cybercriminals presents a concrete risk that the cybercriminals who now possess Class members' Private Information will do so at a later date or re-sell it.

68. Data breaches have also proven to be costly for affected organizations as well, with the average cost to resolve being $4.45 million dollars in 2023.[26] The average cost to resolve a data breach involving health information, however, is more than double this figure at $10.92 million.[27]

69. In response to the Data Breach, Defendants offered to provide certain individuals whose Private Information was exposed in the Data Breach with just 12 months of credit monitoring. However, one year of credit monitoring is much shorter than what is

---

[24] David Burnes, Marguerite DeLiema, Lynn Langton, *Risk and protective factors of identity theft victimization in the United States*, Preventive Medicine Reports, Volume 17 (January 23, 2020), available at https://www.sciencedirect.com/science/article/pii/S2211335520300188?via%3Dihub.

[25] *Id.*

[26] *Cost of a Data Breach Report 2023*, IBM Security, available at https://www.ibm.com/reports/data-breach?utm_content=SRCWW&p1=Search&p4=43700072379268622&p5=p&gclid=CjwKCAjwxOymBhAFEiwAnodBLGiGtWfjX0vRlNbx6p9BpWaOo9eZY1i6AMAc6t9S8IKsxdnbBVeUbxoCtk8QAvD_BwE&gclsrc=aw.ds.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

necessary to protect against the lifelong risk of harm imposed on Plaintiff and Class members by Defendants' failures.

70. Moreover, the credit monitoring offered by Defendants is fundamentally inadequate to protect them from the injuries resulting from the unauthorized access and exfiltration of their sensitive Private Information.

71. Here, due to the Data Breach, Plaintiff and Class members have been exposed to injuries that include, but are not limited to:

a. Theft of Private Information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of financial accounts as a direct and proximate result of the Private Information stolen during the Data Breach;

c. Damages arising from the inability to use accounts that may have been compromised during the Data Breach;

d. Costs associated with spending time to address and mitigate the actual and future consequences of the Data Breach, such as finding fraudulent charges, cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, placing freezes and alerts on their credit reports, contacting their financial institutions to notify them that their personal information was exposed and to dispute fraudulent charges, imposition of withdrawal and purchase limits on compromised accounts, including but not limited to lost productivity and opportunities, time taken from the enjoyment of one's life, and the inconvenience, nuisance, and annoyance of dealing with all issues resulting from the Data Breach;

e. The imminent and impending injury resulting from potential fraud and identity theft posed because their Private Information is exposed for theft and sale on the dark web; and

f. The loss of Plaintiff's and Class members' privacy.

72. Plaintiff and Class members have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from

---

[27] *Id.*

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

their Private Information being accessed by cybercriminals, risks that will not abate within a 12-months: the unauthorized access of Plaintiff's and Class members' Private Information, especially their Social Security numbers, puts Plaintiff and the Class at risk of identity theft indefinitely, and well beyond the limited period of credit monitoring that Defendants offered victims of the Data Breach.

73. As a direct and proximate result of Defendants' acts and omissions in failing to protect and secure Private Information, Plaintiff and Class members have been placed at a substantial risk of harm in the form of identity theft, and they have incurred and will incur actual damages in an attempt to prevent identity theft.

74. Plaintiff retains an interest in ensuring there are no future breaches, in addition to seeking a remedy for the harms suffered as a result of the Data Breach on behalf of both herself and similarly situated individuals whose Private Information was accessed in the Data Breach.

G. EXPERIENCES SPECIFIC TO PLAINTIFF

75. Plaintiff Whitcraft is a former employee of CellNetix Pathology and Laboratories.

76. Plaintiff Whitcraft received notice of the Data Breach from Defendants. The notice informed Plaintiff Whitcraft that her Private Information had been improperly accessed and obtained by third parties, including but not limited her full name, Social Security number, date of birth, driver's license or state identification number, passport number, and health insurance policy or health insurance identification number.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

77. Following the Data Breach, Plaintiff Whitcraft experienced multiple unauthorized attempts to change the mailing address on Plaintiff's financial accounts, and Plaintiff Whitcraft's email account was accessed without her authorization.

78. As a result of the Data Breach and suspicious activities, Plaintiff Whitcraft has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. She has also spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities, including, but not limited to, work and recreation.

79. As a result of the Data Breach, Plaintiff Whitcraft has suffered anxiety due to the public dissemination of her Private Information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and using her private information for purposes of identity theft and fraud. Plaintiff Whitcraft is concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

80. Plaintiff Whitcraft suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Defendants obtained from her; (b) violation of her privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

81. As a result of the Data Breach, Plaintiff Whitcraft anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

by the Data Breach. And, as a result of the Data Breach, she is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

V. CLASS REPRESENTATION ALLEGATIONS

82. Plaintiff brings this action on behalf of herself and, pursuant to CR 23(a), 23(b)(2), and 23(b)(3), a Class of:

> All persons in the United States whose Private Information was accessed in the Data Breach.

Excluded from the Class are Defendants, its executives and officers, and the Judge(s) assigned to this case. Plaintiff reserves the right to modify, change or expand the Class definition after conducting discovery.

83. Numerosity: Upon information and belief, the Class is so numerous that joinder of all members is impracticable with the number of affected individuals estimated to be in the thousands. The exact number and identities of individual members of the Class are unknown at this time, such information being in the sole possession of Defendants and obtainable by Plaintiff only through the discovery process. The members of the Class will be identifiable through information and records in Defendants' possession, custody, and control.

84. Existence and Predominance of Common Questions of Fact and Law: Common questions of law and fact exist as to all members of the Class. These questions predominate over the questions affecting individual Class members. These common legal and factual questions include, but are not limited to:

a. When Defendants learned of the Data Breach;

b. Whether hackers obtained Class members' Private Information via the Data Breach;

c. Whether Defendants' response to the Data Breach was adequate;

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

d. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

e. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations, industry standards, and/or its own promises and representations;

f. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;

g. Whether Defendants owed a duty to Class members to safeguard their Private Information;

h. Whether Defendants breached their duty to Class members to safeguard their Private Information;

i. Whether Defendants' conduct was unfair or deceptive;

j. Whether Defendants' conduct impacts the public interest;

k. Whether Defendants' conduct violated the FTCA, HIPAA, and/or the Consumer Protection Act invoked herein;

l. Whether Defendants' conduct was negligent;

m. Whether Defendants were unjustly enriched;

n. What damages Plaintiff and Class members suffered as a result of Defendants' misconduct;

o. Whether Plaintiff and Class members are entitled to actual and/or statutory damages; and

p. Whether Plaintiff and Class members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

85. Typicality: All of Plaintiff's claims are typical of the claims of the Class because Plaintiff and all members of the Class had their Private Information compromised in the Data Breach. Plaintiff's claims and damages are also typical of the Class because they resulted from Defendants' uniform wrongful conduct. Likewise, the relief to which Plaintiff is entitled is

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

typical of the Class because Defendants have acted, and refused to act, on grounds generally applicable to the Class.

86. Adequacy: Plaintiff is an adequate class representative because her interests do not materially or irreconcilably conflict with the interests of the Class she seeks to represent, she has retained counsel competent and highly experienced in complex class action litigation, and she intends to prosecute this action vigorously. Plaintiff and her counsel will fairly and adequately protect the interests of the Class. Neither Plaintiff nor her counsel have any interests that are antagonistic to the interests of other members of the Class.

87. Superiority: Compared to all other available means of fair and efficient adjudication of the claims of Plaintiff and the Class, a class action is the most superior. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Defendants' conduct. It would be virtually impossible for members of the Class individually to effectively redress the wrongs done to them. Even if the members of the Class could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties and to the court system presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Members of the Class can be readily identified and notified based on, *inter alia*, Defendants' records and databases.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

VI. CAUSES OF ACTION

COUNT I
VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT, RCW 19.86
(By Plaintiff on behalf of the Class)

88. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

89. The Washington State Consumer Protection Act ("CPA") prohibits any "unfair or deceptive acts or practices" in the conduct of any trade or commerce as those terms are defined by the CPA and relevant caselaw. RCW 19.86.020.

90. Defendants are a "person" as defined in RCW 19.86.010(1).

91. Defendants engage in "trade" and "commerce" as defined in RCW 19.86010(2) through the sale of services and commerce that directly and indirectly affects the people of the State of Washington.

92. Based on the above-described wrongful actions, inaction, omissions, and negligent acts that directly and proximately caused the Data Breach, Defendants engaged in unlawful, unfair, and fraudulent practices within the meaning, and in violation of, the CPA.

93. In the ordinary course of business, Defendant committed "unfair or deceptive acts or practices" by, among other things, knowingly failing to ensure the safeguarding and protection of Plaintiffs' and Class Members' Private Information. Plaintiffs and Class Members reserve the right to allege other violations of law by Defendants constituting other unlawful business acts or practices.

94. Defendants also violated the CPA by failing to timely notify and concealing from Plaintiff and Class Members information regarding the unauthorized access of their PII. If

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Plaintiff and Class Members had been notified earlier, and had the information not been concealed, they could have taken precautions to safeguard their PII.

95. As a direct and proximate result of Defendant's above-described wrongful actions, inactions, omissions, and negligent acts, Plaintiff and Class Members have suffered, and will continue to suffer economic damages and other injury and actual harm including, but not limited to: (1) a present and imminent risk of identity theft and identity fraud—risk justifying expenditures for protective and remedial services for which they are entitled compensation; (2) invasion of privacy; (3) breach of the confidentiality of their PII; (4) deprivation of the value of their Private Information, for which there is a well-established national and international market; and (5) the financial and temporal cost of monitoring credit, monitoring financial accounts, and mitigating damages.

96. Unless restrained and enjoined, Defendants will continue to engage in the above-described wrongful conduct and more data breaches will occur. Therefore, Plaintiff, on behalf of herself and Class Members, seek restitution and an injunction prohibiting Defendants from continuing such wrongful conduct, and requiring Defendants to ensure the safeguarding and protection of Plaintiff's and Class Members' Private Information by the entities to whom it provides that information.

97. Plaintiff, on behalf of herself and Class Members, also seek to recover actual damages sustained by each Class Member together with the costs of the suit, including reasonable attorneys' fees and costs. Additionally, Plaintiff on behalf of herself and Class Members request that this Court use its discretion under RCW 19.86.090 to increase the damages award for each Class Member by three times the actual damages sustained, not to exceed $25,000 per Class Member.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

COUNT II
NEGLIGENCE
(By Plaintiff on behalf of the Class)

98. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

99. Defendants owe a duty of care to protect the Private Information belonging to Plaintiff and Class members. Defendants also owe several specific duties including, but not limited to, the duty:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. to protect patients' and employees' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. to have procedures in place to detect the loss or unauthorized dissemination of Private Information in its possession;

d. to employ reasonable security measures and otherwise protect the Private Information of Plaintiff and Class members pursuant to the FTCA;

e. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. to promptly notify Plaintiff and Class members of the Data Breach, and to precisely disclose the type(s) of information compromised.

100. Defendants also owe this duty because Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 requires Defendants to use reasonable measures to protect confidential data.

101. Defendants also owe this duty because industry standards mandate that Defendants protect its patients' and employees' confidential private information.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

102. Defendants also owe this duty because they had a special relationship with Plaintiff and Class members. Plaintiff and Class members entrusted their Private Information to Defendants on the understanding that adequate security precautions would be taken to protect this information. Furthermore, only Defendants had the ability to protect their systems and the Private Information stored on them from attack.

103. Defendants breached their duties to Plaintiff and the Class by failing to take reasonable appropriate measures to secure, protect, and/or otherwise safeguard the Private Information belonging to Plaintiff and Class members.

104. As a direct and proximate result of Defendants' conduct, Plaintiff and the Class were damaged. These damages include, and are not limited to:

- Lost or diminished value of their Private Information;
- Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information;
- Lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges; and
- Permanent increased risk of identity theft.

105. Plaintiff and Class members were foreseeable victims of any inadequate security practices on the part of Defendants and the damages they suffered were the foreseeable result of the aforementioned inadequate security practices.

106. In failing to provide prompt and adequate individual notice of the Data Breach, Defendants also acted with reckless disregard for the rights of Plaintiff and Class members.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

107. Plaintiff and Class members are entitled to damages in an amount to be proven at trial and injunctive relief requiring Defendants to, *inter alia*, strengthen their data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class members.

COUNT III
BREACH OF IMPLIED CONTRACT
(By Plaintiff on behalf of the Class)

108. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

109. Plaintiff and the Class provided Defendants with their Private Information.

110. By providing their Private Information, and upon Defendants' acceptance of this information, Plaintiff and the Class, on one hand, and Defendants, on the other hand, entered into implied-in-fact contracts for the provision of data security, separate and apart from any express contract entered into between the parties.

111. The implied contracts between Defendants and Plaintiff and Class members obligated Defendants to take reasonable steps to secure, protect, safeguard, and keep confidential Plaintiff's and Class members' Private Information. The terms of these implied contracts are described in federal laws, state laws, and industry standards, as alleged above.

112. The implied contracts for data security also obligated Defendants to provide Plaintiff and Class members with prompt, timely, and sufficient notice of any and all unauthorized access or theft of their Private Information.

113. Defendants breached these implied contracts by failing to take, develop and implement adequate policies and procedures to safeguard, protect, and secure the Private Information belonging to Plaintiff and Class members; allowing unauthorized persons to access

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Plaintiff's and Class members' Private Information; and failing to provide sufficient notice of the Data Breach to Plaintiff and Class members, as alleged above.

114. As a direct and proximate result of Defendants' breaches of the implied contracts, Plaintiff and the Class have been damaged as described herein, will continue to suffer injuries as detailed above due to the continued risk of exposure of Private Information, and are entitled to damages in an amount to be proven at trial.

COUNT IV
UNJUST ENRICHMENT
(By Plaintiff on behalf of the Class)

115. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

116. This count is brought in the alternative to Count III.

117. Plaintiff and the Class have a legal and equitable interest in their Private Information that was collected and maintained by Defendants.

118. Defendants were benefitted by the conferral of Plaintiff's and Class members' Private Information and by their ability to retain and use that information. Defendants understood that they were in fact so benefitted.

119. Defendants also understood and appreciated that Plaintiff's and Class members' Private Information was private and confidential and its value depended upon Defendants maintaining the privacy and confidentiality of that information.

120. But for Defendants' willingness and commitment to maintain its privacy and confidentiality, Plaintiff and Class members would not have provided or authorized their Private Information to be provided to Defendants, and Defendants would have been deprived of the competitive and economic advantages they enjoyed by falsely claiming that their data-

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

security safeguards met reasonable standards. These competitive and economic advantages include, without limitation, wrongfully gaining patients, gaining the reputational advantages conferred upon them by Plaintiff and Class members, collecting excessive advertising and sales revenues as described herein, monetary savings resulting from failure to reasonably upgrade and maintain data technology infrastructures, staffing, and expertise raising investment capital as described herein, and realizing excessive profits.

121. As a result of Defendants' wrongful conduct as alleged herein (including, among other things, their deception of Plaintiff, the Class, and the public relating to the nature and scope of the data breach; their failure to employ adequate data security measures; their continued maintenance and use of the Private Information belonging to Plaintiff and Class members without having adequate data security measures; and their other conduct facilitating the theft of that Private Information), Defendants have been unjustly enriched at the expense of, and to the detriment of, Plaintiff and the Class.

122. Defendants' unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff's and Class members' sensitive Private Information, while at the same time failing to maintain that information secure from intrusion.

123. Under the common law doctrine of unjust enrichment, it is inequitable for Defendants to be permitted to retain the benefits they received, and are still receiving, without justification, from Plaintiff and the Class in an unfair and unconscionable manner.

124. The benefit conferred upon, received, and enjoyed by Defendants were not conferred officiously or gratuitously, and it would be inequitable and unjust for Defendants to retain the benefit.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

125. Defendants are therefore liable to Plaintiff and the Class for restitution in the amount of the benefit conferred on Defendants as a result of their wrongful conduct, including specifically the value to Defendants of the Private Information that was accessed and exfiltrated in the Data Breach and the profits Defendants received from the use and sale of that information.

126. Plaintiff and Class members are entitled to full refunds, restitution, and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from their wrongful conduct.

127. Plaintiff and Class members may not have an adequate remedy at law against Defendants, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT V
INVASION OF PRIVACY
(By Plaintiff on behalf of the Class)

128. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

129. Plaintiff and Class members had a reasonable expectation of privacy in the Private Information that Defendants possessed and/or continues to possess.

130. By failing to keep Plaintiff's and Class members' Private Information safe, and by misusing and/or disclosing their Private Information to unauthorized parties for unauthorized use, Defendants invaded Plaintiff's and Class members' privacy by:

a. Intruding into their private affairs in a manner that would be highly offensive to a reasonable person; and

b. Publicizing private facts about Plaintiff and Class members, which is highly offensive to a reasonable person.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

131. Defendants knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiff's position would consider Defendants' actions highly offensive.

132. Defendants invaded Plaintiff's and Class members' right to privacy and intruded into Plaintiff's and Class members' private affairs by misusing and/or disclosing their private information without their informed, voluntary, affirmative, and clear consent.

133. As a proximate result of such misuse and disclosures, Plaintiff's and Class members' reasonable expectation of privacy in their Private Information was unduly frustrated and thwarted. Defendants' conduct amounted to a serious invasion of Plaintiff's and Class members' protected privacy interests.

134. In failing to protect Plaintiff's and Class members' Private Information, and in misusing and/or disclosing their Private Information, Defendants have acted with malice and oppression and in conscious disregard of Plaintiff's and the Class members rights to have such information kept confidential and private, in failing to provide adequate notice, and in placing its own economic, corporate, and legal interests above the privacy interests of its millions of patients. Plaintiff, therefore, seek an award of damages, including punitive damages, on behalf of Plaintiff and the Class.

PRAYER FOR RELIEF

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

A. That the Court certify this action as a class action, proper and maintainable pursuant to CR 23; declare that Plaintiff is a proper class representative; and appoint Plaintiff's Counsel as Class Counsel;

B. That Plaintiff be granted the declaratory relief sought herein;

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

C. That the Court grant permanent injunctive relief to prohibit Defendants from continuing to engage in the unlawful acts, omissions, and practices described herein;

D. That the Court award Plaintiff and the Class members compensatory, consequential, and general damages in an amount to be determined at trial;

E. That the Court award Plaintiff and the Class members statutory damages, including treble damages, to the extent permitted by law;

F. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

G. That the Court award pre- and post-judgment interest at the maximum legal rate;

H. That the Court award grant all such equitable relief as it deems proper and just, including, but not limited to, disgorgement and restitution; and

I. That the Court grant all other relief as it deems just and proper.

Date: February 5, 2024

Respectfully Submitted,

TOUSLEY BRAIN STEPHENS PLLC

By: s/ *Kaleigh N. Boyd*
Kaleigh N. Boyd, WSBA #52684
kboyd@tousley.com
1200 Fifth Avenue, Suite 1700
Seattle, WA 98101
Tel: (206) 682-5600/Fax: (206) 682-2992

Daniel O. Herrera*
Nickolas J. Hagman*
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
Telephone: (312) 782-4880
Facsimile: (312) 782-4485
dherrera@caffertyclobes.com
nhagman@caffertyclobes.com

**pro hac vice to be filed*

Attorneys for Plaintiff and the Proposed Class