UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

E.S., individually and on behalf of all others similarly situated,

Plaintiff,

v.

CHANGE HEALTHCARE INC., CHANGE HEALTHCARE LLC,

Defendants.

Case No. 0:24-cv-4031

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

COMES NOW, Plaintiff, E.S., individually and on behalf of all others similarly situated, and on behalf of the general public, upon personal knowledge of facts pertaining to him and upon information and belief as to all other matters, and by and through undersigned counsel, hereby brings this Class Action Complaint against Defendants, Change Healthcare Inc. and Change Healthcare LLC (or "Defendants"), and alleges as follows:

NATURE OF THE CASE

1. This action brought by Plaintiff and the Class seeks to redress Defendants' willful and reckless violations of their privacy rights. Plaintiff was a client of Defendants who entrusted his Protected Health Information ("PHI") and Personally Identifiable Information ("PII") to Defendants. Defendants betrayed Plaintiff's trust by failing to

properly safeguard and protect his PHI and PII by publicly disclosing his PHI and PII without authorization in violation of Minnesota common law.

2. This action pertains to Defendants' unauthorized disclosure of the Plaintiff's and the Class Members' PHI and PII that occurred on or around February 21, 2024 (the "Breach").

3. Defendants disclosed Plaintiff's and the Class Members' PHI and PII to unauthorized persons as a direct and/or proximate result of Defendants' failure to safeguard and protect their PHI and PII.

4. The wrongfully disclosed PHI and PII included, *inter alia*, Plaintiff's name, address, date of birth, phone number, social security number, drivers license number, email, health insurance data, health data (including medical record numbers, doctors, diagnoses, medications, test results, images, care, and treatment).

5. Defendants flagrantly disregarded Plaintiff's and the Class Members' privacy and property rights by intentionally, willfully and recklessly failing to take the necessary precautions required to safeguard and protect Plaintiff's and the Class Members' PHI and PII from unauthorized disclosure. Plaintiff's and the Class Members' PHI and PII was improperly handled, inadequately protected, and not kept in accordance with basic security protocols. Defendants' obtaining of the information and sharing of same also represent a flagrant disregard of Plaintiff's and the Class Members' rights, both as to privacy and property.

6. Plaintiff has standing to bring this action individually and on behalf of others similarly situated because as a direct and/or proximate result of Defendants' wrongful

actions and/or inaction and the resulting Breach, Plaintiff has incurred (and will continue to incur) damages in the form of, *inter alia*, (i) loss of privacy and/or (ii) the additional damages set forth in detail below, which are incorporated herein by reference.

7. Defendants' wrongful actions and/or inaction and the resulting Breach have also placed Plaintiff and the Class at an imminent, immediate and continuing increased risk of identity theft, identity fraud and medical fraud. Indeed, Javelin Strategy & Research ("Javelin"), a leading provider of quantitative and qualitative research, released its 2012 Identity Fraud Report ("the Javelin Report"), quantifying the impact of breaches. According to the Javelin Report, individuals whose PHI and PII is subject to a reported breach—such as the Breach at issue here—are approximately 9.5 times more likely than the general public to suffer identity fraud and/or identity theft. Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported, and a high probability that criminals who may now possess Plaintiff's and the Class Members' PHI and PII and not yet used the information will do so at a later date or re-sell it.

8. Plaintiff and the Class have also suffered and is entitled to damages for the lost benefit of their bargain with Defendants. Plaintiff and the Class paid Defendants for their services including it protecting their PHI and PII. The lost benefit of the bargain is measured by the difference between the value of what Plaintiff and the Class should have received when they paid for Defendants' services, and the value of what they actually did receive: services without adequate privacy safeguards. Plaintiff and the Class have been harmed in that they (1) paid more for privacy and confidentiality than they otherwise

would have, and (2) paid for privacy protections they did not receive. In that respect, Plaintiff and the Class have not received the benefit of the bargain and has suffered an ascertainable loss.

9. Additionally, because of Defendants' conduct, Plaintiff and the Class have been harmed in that Defendants have breached their common law fiduciary duty of confidentiality owed to Plaintiff and the Class.

10. Accordingly, Plaintiff and the Class seek redress against Defendants for breach of implied contract, breach of contract, common law negligence, breach of the Minnesota Uniform Deceptive Trade Practices Act, negligent training and supervision, negligence *Per Se*, and breach of fiduciary duty of confidentiality.

11. Plaintiff and the Class seek all (i) actual damages, economic damages, (ii) injunctive relief, and (iii) attorneys' fees, litigation expenses, and costs.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d) because there are more than 100 Class Members, at least one class member is a citizen of a state different from that of Defendants, and the amount in controversy exceeds $5 million, exclusive of interest and costs.

13. Venue is likewise proper in this District pursuant to 28 U.S.C. § 1391(b) because Defendants conduct much of their business in this District and Defendants have caused harm to Class Members residing in this District.

14. This case has been consolidated under MDL No. 24-3108 in the District of

Minnesota.

PARTIES

15. Plaintiff is an adult individual residing in Leawood, Johnson County, Kansas.

16. At all relevant times, Defendant Change Healthcare Inc. has been a company which provides health services to Kansas residents. Defendant Change Healthcare Inc.'s headquarters is in Nashville, Tennessee.

17. At all relevant times, Defendant Change Healthcare LLC has been a company which provides health services to Kansas residents. Defendant Change Healthcare Inc.'s headquarters is in Nashville, Tennessee.

BACKGROUND FACTS

18. Certain allegations are made upon information and belief.

19. Defendants provide health care provider support services pursuant to state and federal law, providing health care and medical services to the general public, including Plaintiff and the Class.

20. In the course of these services, Defendants collect and maintain clients' highly sensitive PHI and PII, including, but not limited to, their names, addresses, dates of birth, phone numbers, social security numbers, drivers' license numbers, emails, health insurance data, health data (including doctors, diagnoses, medications, test results, images, care, and treatment).

21. By obtaining, collecting, and storing the PHI and PII of Plaintiff and the Class Members, Defendants assumed legal and equitable duties and knew or should have known it was responsible for protecting the PHI and PII from unauthorized disclosure.

22. Defendants understand the importance of protecting its clients' PHI and PII. Defendants maintains a Privacy Policy confirming such. According to Defendants' Privacy Notice, "We implement and maintain organizational, technical, and administrative security measures designed to safeguard the data we process against unauthorized access, destruction, loss, alteration, or misuse. These measures are aimed at providing on-going integrity and confidentiality of data, including your personal information."[1]

23. As a part of their business operations, Defendants collect and maintain PHI and PII of their clients.

24. Plaintiff was a client of Defendants and, as a result, provided his PHI and PII to Defendants.

25. Plaintiff and the Class Members entered into an implied contract with Defendants for the adequate protection of their PHI and PII.

26. Defendants are required to maintain the strictest privacy and confidentiality of Plaintiff's and the Class Members' medical records and other PHI and PII.

27. In or about February 2024, Plaintiff was a client of Defendants.

28. At no point did Defendants have any authorization from Plaintiff or any order from a Court allowing the disclosure of this highly sensitive medical information to anyone.

[1] https://www.changehealthcare.com/privacy-notice (Last visited August 9, 2024).

29. According to a data breach notice sent by Defendants ("Breach Notice"), cybercriminals accessed certain systems of Defendants' network on or around February 21, 2024, exploiting a glaring vulnerability in the software and downloading highly sensitive PHI PII of all of Defendants' customers stored on its servers, including Social Security numbers, first and last names, dates of birth, driver's license numbers, other state identification numbers, medical claims information, provider information, clinical information, health insurance information, and addresses.

30. The Breach Notice further provided that "[o]n March 7, 2024 we learned a cybercriminal was able to see and take copies of some data in our computer systems."

31. Defendants also posted a Notice of Data Breach ("Cyber Notice") on its website that vaguely discusses the Data Breach and imprecisely addresses the steps taken to ensure a Data Breach of this kind does not happen again.[2]

32. Absent from the Breach Notice and Security Notice are any details regarding how the Data Breach happened, what Defendants did in response to the ransom demand, or how Defendants actions have remediated the root cause of the Data Breach.

33. Defendants' lack of investigation regarding the egregious disclosure of Plaintiff's and the Class Members' highly sensitive medical information is a gross disregard to the Plaintiff's and the Class Members' concerns of their privacy.

34. The disclosure of the PHI and PII at issue was a result of the Defendants' inadequate safety and security protocols governing PHI and PII.

[2] https://www.changehealthcare.com/hipaa-substitute-notice (Last visited on August 9, 2024).

35. The wrongfully disclosed PHI and PII included, *inter alia*, Plaintiff's and the Class Members' names, addresses, dates of birth, phone numbers, social security numbers, drivers' license numbers, email addresses, health insurance data, and health data.

36. As a direct and/or proximate result of Defendants' failure to properly safeguard and protect the PHI and PII of their clients, Plaintiff's and the Class Members' PHI and PII was stolen, compromised, and wrongfully disseminated without authorization.

37. Defendants have a duty to their clients to protect them from wrongful disclosures.

38. As a health care provider, Defendants are required to train and supervise their employees regarding the policies and procedures as well as the State and Federal laws for safeguarding client/patient information.

39. Defendants are covered entities pursuant to the Health Insurance Portability and Accountability Act ("HIPAA"). *See* 45 C.F.R. § 160.102. Defendants must therefore comply with the HIPAA Privacy Rule and Security Rule. *See* 45 C.F.R. Part 160 and Part 164, Subparts A through E.

40. Defendants are covered entities pursuant to the Health Information Technology Act ("HITECH")[3]. *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

41. The HIPAA and HITECH rules work in conjunction with the already established laws of privacy Minnesota. HIPAA and HITECH do not recognize an

[3] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

individual right of claim for violation but provide the guidelines for the standard of procedure dictating how patient medical information should be kept private.

42. HIPAA's Privacy Rule, otherwise known as "Standards for Privacy of Individually Identifiable Health Information," establishes national standards for the protection of health information.

43. HIPAA's Security Rule, otherwise known as "Security Standards for the Protection of Electronic Protected Health Information," establishes national security standards for the protection of health information that is held or transferred in electronic form. *See* 42 C.F.R. §§ 164.302-164.318.

44. HIPAA limits the permissible uses of "protected health information" and prohibits the unauthorized disclosure of "protected health information." 45 C.F.R. § 164.502. HIPAA requires that covered entities implement appropriate administrative, technical, and physical safeguards for this information and requires that covered entities reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart. *See* 45 C.F.R. § 164.530(c).

45. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

46. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health

information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

47. Under HIPAA:

> Protected health information means individually identifiable health information:
>
> (1) Except as provided in paragraph (2) of this definition, that is:
>
> (i) Transmitted by electronic media;
>
> (ii) Maintained in electronic media; or
>
> (iii) Transmitted or maintained in any other form or medium.[4]

48. HIPAA and HITECH obligated Defendants to implement technical policies and procedures for electronic information systems that maintain electronic protected health information so that such systems were accessible only to those persons or software programs that had been granted access rights and who have a working need to access and view the information. *See* 45 C.F.R. § 164.312(a)(1); *see also* 42 U.S.C. §17902.

49. HIPAA and HITECH also obligated Defendants to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

[4] 45 C.F.R. § 160.103

50. HIPAA further obligated Defendants to ensure that their workforce complied with HIPAA security standard rules (*see* 45 C.F.R. § 164.306(a)(4)) to effectively train their workforces on the policies and procedures with respect to protected health information, as necessary and appropriate for those individuals to carry out their functions and maintain the security of protected health information. *See* 45 C.F.R. § 164.530(b)(1).

51. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." *See* US Department of Health & Human Services, Security Rule Guidance Material.[5] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says, "represent the industry standard for good business practices with respect to standards for securing e-PHI." *See* US Department of Health & Human Services, Guidance on Risk Analysis.[6]

52. Should a health care provider experience an unauthorized disclosure, it is required to conduct a Four Factor Risk Assessment (HIPAA Omnibus Rule). This standard

[5] http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html
[6] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

requires, "A covered entity or business associate must now undertake a four-factor risk assessment to determine whether or not PHI has been compromised and overcome the presumption that the breach must be reported. The four-factor risk assessment focuses on:

> (1) the nature and extent of the PHI involved in the incident (e.g., whether the incident involved sensitive information like social security numbers or infectious disease test results);
>
> (2) the recipient of the PHI;
>
> (3) whether the PHI was actually acquired or viewed; and
>
> (4) the extent to which the risk that the PHI was compromised has been mitigated following unauthorized disclosure (e.g., whether it was immediately sequestered and destroyed)."[7]

53. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

54. The HIPAA Contingency Operations Rule, 45 C.F.R. §164.301(a), requires a healthcare provider to have security measures in place and train their employees and staff so that all their staff and employees know their roles in facility security.

55. Defendants failed to provide proper notice to Plaintiff and the Class of the disclosure, first sending notification approximately four (4) months after discovering the breach, on June 20, 2024.

[7] 78 Fed. Reg. 5641-46, *See also*, 45 C.F.R. §164.304

56. Defendants failed to conduct or improperly conducted the four-factor risk assessment following the unauthorized disclosure.

57. Defendants flagrantly disregarded and/or violated Plaintiff's and the Class Members' privacy and property rights, and harmed them in the process, by not obtaining Plaintiff's or the Class Members' prior written consent to disclose their PHI and PII to any other person—as required by laws, regulations, industry standards and/or internal department standards.

58. Defendants flagrantly disregarded and/or violated Plaintiff's and the Class Members' privacy and property rights, and harmed them in the process, by failing to safeguard and protect and, in fact, wrongfully disseminating Plaintiff's and the Class Members' PHI and PII to unauthorized persons.

59. Defendants flagrantly disregarded and/or violated Plaintiff's and the Class Members' privacy rights, and harmed them in the process, by failing to establish and/or implement appropriate administrative, technical and/or physical safeguards to ensure the security and confidentiality of Plaintiff's and the Class Members' PHI and PII to protect against anticipated threats to the security or integrity of such information. Defendants' unwillingness or inability to establish and maintain the proper information security procedures and controls is an abuse of discretion and confirms their intentional and willful failure to observe procedures required by law, industry standards and/or their own internal policies and procedures.

60. Defendants' wrongful actions and/or inaction directly and/or proximately caused the theft and dissemination into the public domain of Plaintiff's and the Class

Members' PHI and PII without their knowledge, authorization and/or consent. As a direct and/or proximate result of Defendants' wrongful actions and/or inaction and the resulting Breach, Plaintiff and the Class have incurred (and will continue to incur) damages in the form of, *inter alia*, (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII (iii) loss of privacy, (iv) humility, (v) embarrassment (vi) the lost benefit of their bargain when they paid for their privacy to be protected and it was not.

CLASS ACTION ALLEGATIONS

61. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action on behalf of herself and the following proposed Nationwide Class, defined as follows:

Nationwide Class

> All persons residing in the United States who are current or former customers of Defendants or any of Defendants' affiliate, parent, or subsidiary, and had their PHI and PII compromised by an unknown third-party cybercriminal as a result of the Data Breach.

In addition, Plaintiff brings this action on behalf of the following proposed Kansas Subclass, defined as follows:

Kansas Subclass

> All persons residing in the State of Kansas who are current or former customers of Defendants or any of Defendants' affiliate, parent, or subsidiary, and had their PHI and PII compromised as a result of the Data Breach.

62. Both the proposed Nationwide Class and the proposed Kansas Subclass will be collectively referred to as the Class, except where it is necessary to differentiate them.

63. Excluded from the proposed Class are any officer or director of Defendants any officer or director of any affiliate, parent, or subsidiary of Defendants; anyone employed by counsel in this action; and any judge to whom this case is assigned, her or her spouse, and members of the judge's staff.

64. **Numerosity.** Members of the proposed Class likely number in the tens of thousands and are thus too numerous to practically join in a single action. Membership in the Class is readily ascertainable from Defendants' own records.

65. **Commonality and Predominance.** Common questions of law and fact exist as to all proposed Class Members and predominate over questions affecting only individual Class Members. These common questions include:

a. Whether Defendants engaged in the wrongful conduct alleged herein;

b. Whether Defendants' inadequate data security measures were a cause of the Data Breach;

c. Whether Defendants owed a legal duty to Plaintiff and the other Class Members to exercise due care in collecting, storing, and safeguarding their PHI and PII;

d. Whether Defendants negligently or recklessly breached legal duties

owed to Plaintiff and the Class Members to exercise due care in collecting, storing, and safeguarding their PHI and PII;

e. Whether Plaintiff and the Class are at an increased risk for identity theft because of the Data Breach;

f. Whether Defendants failed to implement and maintain reasonable security procedures and practices for Plaintiff's and Class Members' PHI and PII in violation Section 5 of the FTC Act;

g. Whether Plaintiff and the other Class Members are entitled to

actual, statutory, or other forms of damages, and other monetary relief; and

h. Whether Plaintiff and the other Class Members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

66. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff individually and on behalf of the other Class Members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

67. **Typicality:** Plaintiff's claims are typical of the claims of the Members of the Class. All Class Members were subject to the Data Breach and had their PHI and PII accessed by and/or disclosed to unauthorized third parties. Defendants' misconduct affected all Class Members in the same manner.

68. **Adequacy of Representation:** Plaintiff is an adequate representative of the Class because their interests do not conflict with the interests of the other Class Members they seek to represent; they have retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and their counsel.

69. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiff and the other Class Members

are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendants, making it impracticable for Class Members to individually seek redress for Defendants' wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

COUNT I
BREACH OF FIDUCIARY DUTY OF CONFIDENTIALITY

70. The preceding factual statements and allegations are incorporated herein by reference.

71. At all times relevant hereto, Defendants owed, and owe, a fiduciary duty to Plaintiff pursuant to Minnesota common law, to keep Plaintiff's medical and other PHI and PII information confidential.

72. The fiduciary duty of privacy imposed by Minnesota law is explicated under the procedures set forth in the Health Insurance Portability and Accountability Act Privacy Rule, including, without limitation the procedures and definitions of 45 C.F.R. §160.103 and 45 C.F.R. §164.530 which requires a covered entity, health care provider, to apply appropriate administrative, technical, and physical safeguards to protect the privacy of patient medical records.

73. Under their fiduciary duty, Defendants must institute safeguards to protect the privacy and security of their clients' medical records and medical information contained in those records.

74. Defendants breached their fiduciary duty to Plaintiff and the Class by disclosing Plaintiff's and the Class Members' PHI and PII to unauthorized third parties .

75. As a direct result of Defendants' breach of fiduciary duty of confidentiality and the disclosure of Plaintiff's and the Class Members' confidential medical information, Plaintiff suffered damages.

76. Defendants' wrongful actions and/or inaction directly and/or proximately caused the theft and dissemination into the public domain of Plaintiff's and the Class Members' PHI and PII without their knowledge, authorization and/or consent. As a direct and/or proximate result of Defendants' wrongful actions and/or inaction and the resulting Breach, Plaintiff and the Class have incurred (and will continue to incur) damages in the form of, *inter alia*, (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII (iii) loss of privacy, (iv) humility, (v) embarrassment (vi) the lost benefit of their bargain when they paid for their privacy to be protected and it was not.

COUNT II
BREACH OF IMPLIED CONTRACT

77. The preceding factual statements and allegations are incorporated herein by reference.

78. Plaintiff and the Class, as part of their agreement with Defendants, provided

Defendants their PHI and PII.

79. In providing such PHI and PII, Plaintiff and the Class entered into an implied contract with Defendants, whereby Defendants became obligated to reasonably safeguard Plaintiff's and the Class Members' PHI and PII.

80. Under the implied contract, Defendants were obligated to not only safeguard the PHI and PII, but also to provide Plaintiff and the Class with prompt, adequate notice of any Breach or unauthorized access of said information.

81. Defendants breached the implied contract with Plaintiff and the Class Members by failing to take reasonable measures to safeguard their PHI and PII by failing to protect Plaintiff and the Class Members' PHI and PII.

82. Defendants' wrongful actions and/or inaction directly and/or proximately caused the theft and dissemination into the public domain of Plaintiff's and the Class Members' PHI and PII without their knowledge, authorization and/or consent. As a direct and/or proximate result of Defendants' wrongful actions and/or inaction and the resulting Breach, Plaintiff and the Class have incurred (and will continue to incur) damages in the form of, *inter alia*, (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII (iii) loss of privacy, (iv) humility, (v) embarrassment (vi) the lost benefit of their bargain when they paid for their privacy to be protected and it was not.

COUNT III
VIOLATIONS OF MINNESOTA UNIFORM DECEPTIVE
TRADE PRACTICES ACT, MINN. STAT. SEC. 43, et seq.

83. The preceding factual statements and allegations are incorporated herein by reference.

84. Minn. Stat. 325F § 1 prohibits the use of, "[t]he act, use, or employment by any person of any fraud, unfair or unconscionable practice, false pretense, false promise, misrepresentation, misleading statement or deceptive practice, with the intent that others rely thereon in connection with the sale of any merchandise, whether or not any person has in fact been misled, deceived, or damaged thereby…"

85. An "unfair practice" is defined by Minnesota law, Minn. Stat. 325F § 8, as any practice which either-

> (1) offends public policy as established by the statutes, rules, or common law of Minnesota;
>
> (2) is unethical, oppressive, or unscrupulous; or
>
> (3) is substantially injurious to consumers.

86. Plaintiffs and Defendants are "persons" within the meaning of Minn Stat. Sec. 43, et seq.

87. Merchandise is defined by the MUDTPA, to include the providing of "services" and, therefore, encompasses healthcare services. Healthcare services are a good.

88. Efforts to maintain the privacy and confidentiality of medical records are part of the healthcare services associated with a good.

89. Maintenance of medical records are "merchandise" within the meaning of section Minn. Stat. Sec. 43, et seq.

90. Plaintiff's and the Class Members' goods and services purchased from Defendants were for "personal, family or household purposes" within the meaning of the MUDTPA.

91. As set forth herein, Defendants' acts, practices and conduct violate section Minn. Stat. Sec. 43, et seq. in that, among other things, Defendants have used and/or continues to use unfair practices, concealment, suppression and/or omission of material facts in connection with the advertising, marketing, and offering for sale of services associated with healthcare services. Such acts offend the public policy established by Minnesota statute and constitute an "unfair practice" as that term is used in Minn. Stat. 325F § 8.

92. Defendants' unfair, unlawful, and deceptive acts, practices and conduct include: (1) representing to their clients that it will not disclose their sensitive personal health information to an unauthorized third party or parties; (2) failing to implement security measures such as securing the records in a safe place; (3) failing to train personnel; and (4) charging clients for privacy services which were not provided.

93. Defendants' conduct also violates the enabling regulations for the MUDTPA because it: (1) offends public policy; (2) is unethical, oppressive and unscrupulous; (3) causes substantial injury to consumers; (4) it is not in good faith; (5) is unconscionable; and (6) is unlawful. *See* Minn. Stat. Sec. 43, et seq.

94. As a direct and proximate cause of Defendants' unfair and deceptive acts, Plaintiff and the Class Members suffered damages in that they (1) paid more for medical record privacy protections than they otherwise would have, and (2) paid for medical record privacy protections that they did not receive. In this respect, Plaintiff and the Class Members have not received the benefit of the bargain and has suffered an ascertainable loss.

95. Plaintiff and the Class seek actual damages for all monies paid to Defendants in violation of the MUDTPA. In addition, Plaintiff and the Class seek attorneys' fees.

COUNT IV
NEGLIGENCE

96. The preceding factual statements and allegations are incorporated herein by reference.

97. Defendants owed a duty to Plaintiff and the Class Members to safeguard and protect their PHI and PII.

98. Defendants breached their duty by failing to exercise reasonable care and failing to safeguard and protect Plaintiff's and the Class Members' PHI and PII.

99. It was reasonably foreseeable that Defendants' failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class Members' PHI and PII would result in an unauthorized third-party gaining access to such information for no lawful purpose.

100. Defendants' wrongful actions and/or inaction directly and/or proximately caused the theft and dissemination into the public domain of Plaintiff's and the Class

Members' PHI and PII without their knowledge, authorization and/or consent. As a direct and/or proximate result of Defendants' wrongful actions and/or inaction and the resulting Breach, Plaintiff and the Class have incurred (and will continue to incur) damages in the form of, *inter alia*, (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII (iii) loss of privacy, (iv) humility, (v) embarrassment (vi) the lost benefit of their bargain when they paid for their privacy to be protected and it was not.

101. Defendants' wrongful actions and/or inaction and the resulting Breach (as described above) constituted (and continue to constitute) negligence at common law.

COUNT V
NEGLIGENT TRAINING AND SUPERVISION

102. The preceding factual statements and allegations are incorporated herein by reference.

103. At all times relevant hereto, Defendants owe a duty to Plaintiff and the Class to hire competent employees, and to train and supervise them to ensure they recognize the duties owed to their clients.

104. Defendants breached their duty to Plaintiff and the Class by allowing a cybercriminal to have access to medical records and information to unauthorized users.

105. Defendants' wrongful actions and/or inaction directly and/or proximately caused the theft and dissemination into the public domain of Plaintiff's and the Class Members' PHI and PII without their knowledge, authorization and/or consent. As a direct and/or proximate result of Defendants' wrongful actions and/or inaction and the resulting

Breach, Plaintiff and the Class have incurred (and will continue to incur) damages in the form of, *inter alia*, (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII (iii) loss of privacy, (iv) humility, (v) embarrassment (vi) the lost benefit of their bargain when they paid for their privacy to be protected and it was not.

COUNT VI
NEGLIGENCE *PER SE*

106. Plaintiff and the Class incorporate by reference and re-alleges all paragraphs previously alleged herein

107. Defendants are covered entities for purposes of HIPAA.

108. Plaintiff is a member of the class HIPAA and HITECH were created to protect.

109. Plaintiff's and the Class Members' private health information is the type of information HIPAA and HITECH were created to protect. HIPAA and HITECH were created to protect against the wrongful and unauthorized disclosure of an individual's health information.

110. The Defendants gave protected medical information, names, addresses, dates of birth, phone numbers, social security numbers, health insurance data, and health data to an unauthorized third party or unauthorized third parties without the written consent or authorization of Plaintiff.

111. The Defendants gave protected medical information to unauthorized third parties without Plaintiff's and/or the Class Members' oral consent or written authorization.

112. The information disclosed to an unauthorized third party or unauthorized third parties included private health information about medical treatment.

113. The Defendants' disclosure of the private health information of Plaintiff and the Class without consent or authorization is a violation of HIPAA and HITECH and is negligence *per se*.

114. Alternatively, Defendants violated HIPAA and HITECH in that it did not reasonably safeguard the private health information of Plaintiff and the Class from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements pursuant to HIPAA and HITECH including, but not limited to, 42 C.F.R. §§ 164.302-164.318, 45 C.F.R. § 164.500, *et seq*, and 42 U.S.C. §17902, and was therefore negligent *per se*.

115. Defendants' wrongful actions and/or inaction directly and/or proximately caused the theft and dissemination into the public domain of Plaintiff's and the Class Members' PHI and PII without their knowledge, authorization and/or consent. As a direct and/or proximate result of Defendants' wrongful actions and/or inaction and the resulting Breach, Plaintiff and the Class have incurred (and will continue to incur) damages in the form of, *inter alia*, (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII (iii) loss of privacy, (iv) humility, (v) embarrassment (vi) the lost benefit of their bargain when they paid for their privacy to be protected and it was not.

116. Plaintiff and the Class seek actual damages for all monies paid to Defendants in violation of the HIPAA and HITECH. In addition, Plaintiff and the Class seek attorneys' fees.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff and the Class respectfully request that the Court enter judgment in their favor and against Defendants, as follows:

A. Declaring that Defendants breached their fiduciary duty to Plaintiff and Class Members;

B. Declaring that Defendants breached their implied contract with Plaintiff and Class Members;

C. Declaring that Defendants violated the Minnesota Uniform Deceptive Trade Practices Act;

D. Declaring that Defendants negligently disclosed Plaintiff's and the Class Members' PHI and PII;

E. Declaring that Defendants were negligent by negligently training and supervising their employees;

F. Declaring that Defendants were negligent *per se;*

G. Ordering Defendants to pay actual damages to Plaintiff and the Class;

H. For an Order enjoining Defendants from continuing to engage in the unlawful business practices alleged herein;

I. Ordering Defendants to pay attorneys' fees and litigation costs to Plaintiff and the Class;

J. Ordering Defendants to pay both pre- and post-judgment interest on any amounts awarded; and

K. Ordering such other and further relief as may be just and proper.

JURY DEMAND

Plaintiff and the Class respectfully demand a trial by jury on all of their claims and causes of action so triable.

Dated: October 25, 2024

Respectfully submitted,

By:/s/ *Karen Hanson Riebel*

Karen Hanson Riebel (MN #0219770)
Kate M. Baxter-Kauf (MN #0392037)
Emma Ritter Gordon (MN #0404000)
LOCKRIDGE GRINDAL NAUEN PLLP
100 Washington Ave S., Suite 2200
Minneapolis, MN 55401
T : (612) 339-6900
khriebel@locklaw.com
kmbaxter-kauf@locklaw.com
erittergordon@locklaw.com

Maureen M. Brady (*pro hac vice forthcoming*)
Lucy McShane (*pro hac vice forthcoming*)
MCSHUNE & BRADY, LLC
4006 Central Street
Kansas City, MO 6411
T: (816) 888-8010
mbrady@mcshanebradylaw.com
lmcshane@mcshanebradylaw.com

Attorneys for Plaintiff and the Proposed Class