UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

ROBERT MACKEY, on behalf of himself individually and on behalf of all others similarly situated, Plaintiff, v. UNITEDHEALTH GROUP INCORPORATED; UNITEDHEALTHCARE INC.; OPTUM, INC.; and CHANGE HEALTHCARE INC.,	Case No. CLASS ACTION COMPLAINT JURY TRIAL DEMANDED

INTRODUCTION AND SUMMARY OF ACTION

1. Plaintiff Robert Mackey ("Mackey"), on behalf of himself and all others similarly situated, alleges the following against Defendants UnitedHealth Group Incorporated, UnitedHealthcare, Inc., Optum, Inc., and Change Healthcare Inc. (collectively, "Defendants").

2. This class action is brought on behalf of patients whose sensitive personal information was stolen by cybercriminals in a cyber-attack that accessed patient data through Change Healthcare's services on or around February 21, 2024 (the "Data Breach").

3. The Data Breach has affected countless millions of individuals across the country, though at this time it is unknown how many individuals' data has been compromised.[1] Issues related to the Data Breach are ongoing.

[1] Devna Bose, A large US health care tech company was hacked. It's leading to billing delays and security concerns
(Last accessed: March 1, 2024) https://apnews.com/article/change-cyberattack-hospitals-pharmacy-alphv-unitedhealthcare-521347eb9e8490dad695a7824ed11c414

4. Plaintiff unsuccessfully attempted to use his health insurance to fill two prescriptions for medication. Due to Defendant's networks being down at that time, Plaintiff would have had to pay full price for his medication and pursue an insurance claim after the fact.

5. Defendants store a tremendous amount of Plaintiff's PII, including his name, birth date, billing and mailing address, prescriptions, financial information, treatment history, and Social Security number. Presumably, this information has been compromised for Plaintiff and Class Members.

6. As of March 5, 2024, Defendant have yet to notify Plaintiff or provide any information on mitigating the fallout of this Data Breach.

7. Change Healthcare and associated entities, as medical industry experts, knew and should have known how to prevent a common cyberattack.

8. If Plaintiff knew his PII would have been improperly handled, he would have refused to share PII with Defendants.

9. Accordingly, Plaintiff asserts claims for violations of negligence, negligent misrepresentation, breach of contract, breach of implied contract, and unjust enrichment/quasi-contract.

PARTIES

10. Plaintiff Robert Mackey is a resident of California. Mackey's PII is stored and handled by Defendants.

11. Defendant Change Healthcare, LLC is a limited liability company that provides healthcare IT services, including security consulting and risk management. Change Healthcare Technology, LLC's principal place of business is 424 Church St. Suite 1400 Nashville, TN,

37219. Change Healthcare is owned by UnitedHealth Group Incorporated, which is headquartered in Minneapolis, MN.

12. Defendant UnitedHealthcare, Inc. is a Delaware corporation with its principal place of business in Minnetonka, Minnesota.

13. Defendant Optum, Inc. is a Delaware corporation with its principal place of business in Eden Prairie, Minnesota.

JURISDICTION AND VENUE

14. The Court has jurisdiction over Plaintiffs' claims under 28 U.S.C. § 1332(d)(2) ("CAFA"), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendants' citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

15. The Court has personal jurisdiction over Defendants because UnitedHealthcare Inc, Optum Inc. and Change Healthcare are each owned by UnitedHealth Group Incorporated. UnitedHealth Group Incorporated is headquartered in this district. This Court has general and specific jurisdiction because UnitedHealth Group Incorporated has its corporate headquarters in Minnesota.

16. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) because Defendant UnitedHealth Group Incorporated maintains its principal place of business in this District and therefore resides in this District pursuant to 28 U.S.C. § 1391(c)(2). A substantial part of the events or omissions giving rise to the Class's claims also occurred in this District.

STATEMENT OF FACTS

A. Defendants Presented themselves as Healthcare Industry Experts, But Failed to Maintain Reasonable and Adequate Security Measures to Safeguard Patients' Private Information

17. Change Healthcare operates a platform that allows integration and connectivity between patients, providers, and insurers. Change Healthcare stores a vast amount of personally identifiable information ("PII") as part of its business model.

18. Optum Inc. is a provider of pharmacy management and medical administrative services to physicians, hospitals, government entities, health plans, and various related companies, reaching over 100 million consumers every year.[2]

19. October 2022 saw the acquisition of Change Healthcare by UnitedHealth Group. UnitedHealth Group undertook this acquisition in order to merge Optum Inc. with Change Healthcare. Optum's website states that "The combined businesses share a vision for achieving a simpler, more intelligent and adaptive health system for patients, payers and care providers. Optum is focused on connecting and simplifying the core clinical, administrative and payment processes health care providers and payers depend on to serve patients."[3]

20. As part of their regular business operations, Defendants were entrusted with, and obligated to safeguard and protect PII of Plaintiff and the Class in accordance with all applicable laws.

21. The Data Breach occurred on or around February 21, 2024 and is believed to still be ongoing.

---

[2] *Optum: Technology and data-enabled care delivery*, UNITEDHEALTH GROUP, https://www.unitedhealthgroup.com/people-and-businesses/businesses/optum.html (last visited Mar. 5, 2024).

[3] *Change Healthcare is now a part of Optum,* CHANGE HEALTHCARE, https://www.changehealthcare.com/optum (last visited March 5, 2024).

22. In February 2024, Change Healthcare confirmed that a cyberattack had compromised its systems. Plaintiff's information has presumably been compromised. The extent of compromise PII is unknown but likely includes patients' social security numbers, dates of birth, full or partial names, patient biometric data, telephone numbers, mailing and billing addresses, email addresses, patient and record identifiers, information relating to patient treatment (including billing and diagnosis codes, and the dates and locations of treatment), information contained within state-issued photo identification (including driver's license number, organ donor status, and appearance), and insurance cards containing name and/or beneficiary number.

B. Plaintiff and Class Members Suffered Damages

23. Despite holding itself out as holding expertise in healthcare IT, Change Healthcare did not take sufficient security measures for patient PII.

24. Mackey has been unable to timely fill two prescriptions at this point. Providers told him that he could pay full price for these prescriptions, depriving him of his insurance benefits. Mackey is hesitant to pursue further medical care until he is assured that his information has been secured and his insurance coverage will be accepted.

24. Mackey obtained services from Defendant Change Healthcare assuming he would receive the benefit of the bargain in adequate data security of his health information. Yet Change Healthcare has yet to notify Mackey of the extent of his PII that has been compromised. Change Healthcare has not provided any suggestions to Mackey for mitigating the damage he suffers.

25. If Mackey was told that Change Healthcare, his healthcare provider's business associate, failed to maintain adequate computer systems and basic data security practices to

safeguard his PII from a ransomware attack, Mackey would have obtained medical services elsewhere.

C. Defendants Failed to Remedy Harm to Individual Patients from Data Breach

26. Both prior to and after the breach, Defendants advertised themselves on their respective websites as HIPPA compliant.

27. Defendants have yet to affirmatively notify impacted patients individually regarding which specific data was stolen.

28. The Data Breach occurred because Defendants failed to take reasonable measures to protect the PII collected. Change Healthcare failed to implement data security measures designed to prevent this common attack, despite repeated warnings to the healthcare industry about cyberattack risks and the highly publicized occurrence of many similar ransomware attacks in the recent past on other healthcare providers. Defendants failed to disclose to Plaintiff and Class members the material fact that it did not have adequate data security practices to safeguard patients' personal data, and falsely represented that their security measures were sufficient to protect the PII in its possession.

29. Defendants' failure to provide specific resolution of the Breach to Plaintiffs and Class members continues to exacerbate the injuries resulting from the Breach.

D. The Healthcare Industry is the Top Target for Cyber Criminals, and Defendants Failed to Comply with Existing Industry Standards

30. Ransomware attacks have been a well-known risk for healthcare providers for over a decade.

31. In 2020, the Ponemon Institute, one of the leading experts in cybersecurity research, released that the Healthcare industry was the most lucrative target for Data Breaches.[4]

32. The National Institute of Standards & Technology ("NIST") and HIPPA have both had their frameworks readily available, as advertised by the Department of Health and Human Services as a NIST-HIPPA crosswalk framework[5] since before 2016, to follow cybersecurity best practices for healthcare providers that included asset management, access control, and detection processes, as well as other steps that Defendatns took after the data breach, rather than before.

CLASS ACTION ALLEGATIONS

33. Plaintiffs bring all counts, as set forth below, individually and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure, on behalf of a Nationwide Class defined as:

> All persons who submitted their Private Information to Defendants or Defendants' associates and whose Private Information was compromised as a result of the data breach discovered in or about February 2024 (the "Nationwide Class").

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

---

[4] IBM, *How Much Would a Data Breach Cost Your Business?* https://www.ibm.com/security/data-breach

[5] HHS, *Addressing Gaps in Cybersecurity: OCR Releases Crosswalk Between HIPAA Security Rule and NIST Cybersecurity Framework* (Last reviewed February 23, 2016). https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf.

35. ***Numerosity***—Federal Rule of Civil Procedure 23(a)(1). The members of the Class are so numerous that joinder of all Class members would be impracticable. On information and belief, the Nationwide Class numbers in the hundreds of thousands.

36. ***Commonality and Predominance***—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3). Common questions of law and fact exist as to all members of the Class and predominant over questions affecting only individual members of the Class. Such common questions of law or fact include, *inter alia*:

a. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, *e.g.,* HIPAA;

b. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

c. Whether Defendants' properly implemented their purported security measures or their associate's purported security measures to protect Plaintiffs' and the Class's Private Information from unauthorized capture, dissemination, and misuse;

d. Whether Defendants' took reasonable measures to determine the extent of the Data Breach after they first learned of same;

e. Whether Defendants disclosed Plaintiff's and the Class's Private Information in violation of the understanding that the Private Information was being disclosed in confidence and should be maintained;

f. Whether Defendants' conduct constitutes breach of an implied contract;

g. Whether Defendants willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiffs' and the Class's Private Information;

h. Whether Defendants were negligent in failing to properly secure and protect Plaintiffs' and the Class's Private Information;

i. Whether Defendants were unjustly enriched by their actions; and

j. Whether Plaintiff and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of himself and other members of the Class. Similar or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

37. ***Typicality***—Federal Rule of Civil Procedure 23(a)(3). Plaintiffs' claims are typical of the claims of the other members of the Class, because among other things, all Class members were similarly injured through Defendants' uniform misconduct described above and were thus all subject to the Data Breach alleged herein. Further, there are no defenses available to Defendants that are unique to Plaintiffs.

38. ***Adequacy of Representation***—Federal Rule of Civil Procedure 23(a)(4). Plaintiff is an adequate representative of the Nationwide Class because his interests do not conflict with the interests of the Classes they seek to represent, they have retained counsel competent and experienced in complex class action litigation, and Plaintiffs will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiffs and their counsel.

39. ***Injunctive Relief***-Federal Rule of Civil Procedure 23(b)(2). Defendants have acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2).

40. ***Superiority***—Federal Rule of Civil Procedure 23(b)(3). 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 class action. The damages or other financial detriment suffered by Plaintiffs and the other members of the Class are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for members of the Class to individually seek redress for Defendants' wrongful conduct. Even if members of the Class could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases 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 a single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
Negligence

41. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

42. Defendants owed numerous duties to Plaintiff and the Class, including the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting PII in their possession;

b. to protect PII using reasonable and adequate security procedures, systems, and resolutions that are compliant with industry-standard practices;

c. not to subject Plaintiff and the Class's PII to an unreasonable risk of exposure and theft because Plaintiff and Class were foreseeable and probable victims of any inadequate security practices.

d. to use reasonable security measures arose as a result of the special relationship that existed between Defendants and patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law.

43. Upon Defendants accepting and storing the Private Information of Plaintiffs and the Class in their computer systems and on their networks, Defendants undertook and owed a heightened duty to Plaintiffs and the Class to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Change Healthcare knew that the PII was private and confidential and should be protected as private and confidential. Change Healthcare's storage of Plaintiff's PII after Plaintiff's visit was not used to contribute to patients' medical treatment.

44. Change Healthcare's duty to use reasonable security measures under HIPAA required Change Healthcare to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

45. In addition, Change Healthcare had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted, and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

46. Change Healthcare's violation of the FTC Act and state data security statutes constitutes negligence *per se* for purposes of establishing the duty and breach elements of Plaintiffs' negligence claim. Those statutes were designed to protect a group to which Plaintiffs belong and to prevent the type of harm that resulted from the Data Breach.

47. State statutes requiring reasonable data security measures, including but not limited to Minn. R. 325E.61 requiring Defendants to "disclosure must be made in the most expedient time possible and without unreasonable delay" as well as notifying all consumer reporting agencies.

48. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because cybersecurity and healthcare industry standards bound Change Healthcare and other Defendants to protect confidential PII.

49. Change Healthcare's own conduct also created a foreseeable risk of harm to Plaintiffs and Class members and their PII. Change Healthcare's misconduct included failing to: (1) secure Plaintiffs' and Class members' PII; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; (4) respond to security alerts in a timely manner and (5) implement the systems, policies, and procedures necessary to prevent this type of data breach. Defendants were in a special position, with Change Healthcare as an advertised cybersecurity expert, to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class members from a data breach.

50. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Class members' PII. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class members' PII;

b. Failing to adequately monitor the security of Change Healthcare's networks and systems;

c. Allowing unauthorized access to Class members' PII;

d. Failing to resolve in a timely manner that Class members' PII had been compromised; and

e. Failing to offer a protection to Class members to mitigate the potential for identity theft and other damages.

But for Change Healthcare's breach of duties, consumers' PII would not have been stolen.

51. Through Change Healthcare's acts and omissions described in this Complaint, including their failure to provide adequate security and their failure to protect Plaintiffs' and Class members' PII from being foreseeably captured, accessed, disseminated, stolen and misused, Change Healthcare unlawfully breached their duty to use reasonable care to adequately protect and secure Plaintiffs' and Class members' PII during the time it was within Defendants' possession or control.

52. Change Healthcare's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to, failing to adequately protect the PII.

53. Plaintiffs and Class members had no ability to protect their PII once it was in Change Healthcare's possession and control. Change Healthcare was in an exclusive position to protect against the harm suffered by Plaintiffs and Class members as a result of the Data Breach.

54. Neither Plaintiff nor the other Class members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

55. There is a temporal and close causal connection between Change Healthcare's failure to implement adequate data security measures, the Data Breach, and the harms suffered by Plaintiffs and Class members.

56. Plaintiffs and Class members are also entitled to injunctive relief requiring Change Healthcare to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide free credit monitoring and compensation for harm to all Class members.

COUNT II
Negligent Misrepresentation

57. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully set forth herein.

58. As mentioned above, Defendants owed Plaintiff a duty of care to secure Plaintiff's PII.

59. Change Healthcare falsely portrayed itself as HIPPA compliant, with systems that secured patient PII.

60. Plaintiff relied on Change Healthcare's portrayal of adequate security when accepting healthcare services. Plaintiff would not have sought healthcare services but-for portrayal that the healthcare provider's business associate, Change Healthcare, was obliged to protect the privacy of patient information.

61. Defendants failed to disclose to Plaintiffs and Class members that they did not employ reasonable safeguards to protect consumers' PII.

62. Defendants' omissions were made for the guidance of patients in their transactions healthcare business associates, in the course of Defendants' business.

63. Defendants failed to disclose facts or risks which induced patients to act or refrain from acting in their medical transactions.

64. Defendants knew that their data security practices were deficient. Defendants were aware that the health industry was a frequent target of sophisticated cyberattacks. Defendants knew or should have known that their data security practices were insufficient to guard against those well-known ransomware attacks.

65. Defendants were in a special relationship with, or relationship of trust and confidence relative to, patients. Defendants were in an exclusive position to ensure that its safeguards were sufficient to protect against the foreseeable risk that a data breach could occur. Defendants were also in exclusive possession of the knowledge that their data security processes and procedures were inadequate to safeguard consumers' PII.

66. Defendants' omissions were material given the sensitivity of the PII maintained by Defendants and the gravity of the harm that could result from theft of the PII as sensitive and invasive as medical identifiers, social security numbers, biometric information, and more.

67. Data security was an important part of the substance of the transactions and communication between Defendants and patients.

68. Defendants knew that patients would enter transactions under a mistake as to facts basic to the transactions. Because of the relationship between the parties, patients would reasonably expect a disclosure of the basic facts regarding Defendants' data security.

69. If Change Healthcare disclosed to Plaintiff and Class members that its systems were not secure and thus vulnerable to attack, Plaintiff and Class members would not have entrusted their PII to their healthcare providers.

70. In addition to its omissions, Defendants are also liable for implied misrepresentations. Defendants required patients to provide their PII for patients to access medical care. Patient was unaware of Defendants' role in taking Plaintiff's PII. In accepting patient PII, Defendants made implied or implicit representations that they employed reasonable data security practices to protect consumers' PII. This constituted a negligent misrepresentation.

71. Change Healthcare failed to exercise reasonable care or competence in communicating its omissions and misrepresentations.

72. As a direct and proximate result of Defendants' omissions and misrepresentations, Plaintiff and Class members suffered the various types of damages alleged herein. Plaintiff and Class members are entitled to all forms of monetary compensation and injunctive relief set forth herein.

COUNT III
Breach of Contract

73. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

74. Change Healthcare entered into an express agreement as business associates with healthcare providers. Patients, including Plaintiff, were intended beneficiaries in these agreements, as assumed through promise of compliance with HIPPA and industry standards. Plaintiff and Class members justifiably relied on Change Healthcare's promise to protect Plaintiff and Class member's PII.

75. As detailed above, Change Healthcare has a contractual obligation to maintain the security of patients' personal, health, and financial information, which Plaintiff's healthcare provider recognizes in its Notice of Privacy Practices where it addresses, "All of our business

associates are obligated to protect the privacy of your information and abide by the same HIPAA Privacy standards as outlined in this Notice of Privacy Practice." The Notice of Privacy Practice "also describes [patient] rights to access and control your protected health information." Patient's lost control of their data once the Data Breach occurred.

76. In consideration of Plaintiff's agreement to accept medical treatment and make payment for healthcare services rendered, Defendants expressly and/or implicitly agreed to reasonably protect Plaintiff's sensitive personal data and confidential health information as detailed above.

77. The privacy policy also specifically promised the patient that PII did not include dissemination of Personal Information to third-parties as insecure.

78. Defendants breached these contractual obligations by failing to safeguard and protect the PII of Plaintiff and Class members, including through the dissemination of PII through unsecured third-party communication and through PII disclosure, including personal, health, and financial information.

79. Defendants solicited Plaintiffs' sensitive personal data and confidential health information with the express and/or implied understanding that Defendants would safeguard said information from unauthorized cyber-attacks.

80. Plaintiff reasonably believed and expected, in entering said agreements, that Change Healthcare's data security policies, practices and controls would comply with industry standards and applicable laws and regulations, including HIPAA.

81. At all relevant times, Plaintiff fully performed his respective obligations under the parties' agreements.

82. Change Healthcare also breached its contractual obligations by failing to mitigate or resolve patient's personal, health, and/or financial information that was compromised in and as a result of the Breach.

83. The acts and omissions of Change Healthcare constitute a breach of said express and/or implied agreements, all to the damage and pecuniary detriment of Plaintiff without any breach on the part of Plaintiff.

84. The losses and damages sustained by Plaintiff and Class members as described herein were the direct and proximate result of the breaches of the contracts between Defendants and Plaintiff and members of the Class.

85. As a direct and proximate result of the foregoing, Plaintiff and the Class Members have been injured are entitled to damages in an amount to be determined at trial, including, but not limited to, damages via benefit of the bargain, monetary damages and expenses for identity theft protection services and credit monitoring, periodic credit reports, decreased credit score and resulting harm, loss of time, anxiety, emotional distress, loss of privacy and other ordinary, loss of value, incidental and consequential damages as would be anticipated to arise under the circumstances.

86. Plaintiff further seek declaratory and injunctive relief: (1) compelling a security audit of Defendants' electronic computer systems; (2) compelling Defendants to provide Plaintiff and Class members with identity theft protection services and credit monitoring; and (3) compelling Defendants to implement adequate data security safeguards to protect plaintiffs and the class's Personal and Health Information and to undergo future data security audits.

COUNT IV
Breach of Implied Contract

87. Plaintiff re-alleges and incorporate by reference all preceding allegations as if fully set forth herein.

88. When Plaintiff and Class members provided consideration and PII to Defendants in exchange for medical treatment, they entered implied contracts with Defendants under which Defendants agreed to adopt reasonable safeguards complying with relevant laws, regulations, and industry practices, including HIPPA, to protect their PII.

89. Plaintiffs and Class members were required to provide their PII as a condition of the medical treatment.

90. When entering implied contracts, Plaintiff and Class members reasonably believed and expected that Defendants would implement reasonable data security measures and that Defendants' data security practices complied with relevant laws, regulations, and industry standards. Defendants knew or should have known that Plaintiff and Class members held this belief and expectation.

91. Class members who paid money or authorized insurance payments to healthcare provider reasonably believed and expected their business associates would use part of those funds to obtain adequate data security during treatment. As a business associate, Change Healthcare failed to do so.

92. When entering the implied contracts, Defendants impliedly promised to adopt reasonable data security measures. Change Healthcare required taking patient PII for patients to receive medical treatment. In accepting PII, Defendants made implied or implicit promises that its data security practices were reasonably sufficient to protect consumers' PII.

93. Defendants' conduct in requiring patients to provide PII as a prerequisite to their medical treatment illustrates Defendants' intent to be bound by an implied promise to adopt reasonable data security measures.

94. Plaintiff and Class members would not have provided their PII to Defendants in the absence of Defendants' implied promise to keep the PII reasonably secure.

95. Plaintiff and Class members fully performed their obligations under their implied contracts with Defendants. They provided consideration and their PII to Defendants in exchange for medical services and Defendants' implied promise to adopt reasonable data security measures.

96. Defendants breached the implied contract with Plaintiff and Class members by failing to implement reasonable data security measures.

97. As a result of Change Healthcare's conduct, Plaintiff and Class members have suffered, and continue to suffer, legally cognizable damages set forth herein, including nominal damages.

98. Plaintiff and Class members are entitled to all forms of monetary compensation and injunctive relief set forth herein.

99. As a direct and proximate result of Change Healthcare's breaches of the implied contracts between Change Healthcare, Plaintiff and Class members, the Plaintiff and Class members sustained actual losses and damages as described in detail above.

100. Plaintiff and Class members are also entitled to injunctive relief requiring Defendants to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide free credit monitoring to all Class members.

COUNT V
Unjust Enrichment/Quasi-Contract

101. Plaintiff and Class members re-allege and incorporate by reference all preceding allegations as if fully set forth herein.

102. This claim is pled in the alternative to Plaintiff's breach of implied contract claim.

103. Plaintiff and Class members conferred benefits upon Change Healthcare.

104. In exchange for providing payment and PII, Plaintiff and Class members should have received medical treatment accompanied by Defendants' adequate safeguarding of their PII.

105. Change Healthcare knew that Plaintiff and Class members conferred a benefit on it and accepted, has accepted, or retained that benefit. Change Healthcare profited from Plaintiffs' payments and used Plaintiffs' and Class members' Private Information for business or business associate purposes. Change Healthcare had enough revenue to pay attackers. Yet, Change Healthcare still did not compensate the victims of the Data Breach.

106. Change Healthcare's business associate contract with Plaintiff's healthcare provider created Plaintiff and Class members into an implied third-party beneficiary.

107. Change Healthcare failed to secure Plaintiffs' and Class members' PII and, therefore, did not provide full compensation for the benefit the Plaintiffs' and Class members' PII provided.

108. Change Healthcare acquired the PII through inequitable means as they failed to disclose the inadequate security practices previously alleged.

109. If Plaintiff and Class members knew that Change Healthcare would not secure their PII using adequate security, they would not have made transactions with Defendants.

110. Under the circumstances, it would be unjust for Change Healthcare to be permitted to retain

any of the benefits that Plaintiff and Class members conferred on them.

111. Under principles of equity and good conscience, Change Healthcare should not be permitted to retain the full monetary benefit of its transactions with Plaintiffs and Class members. Change Healthcare failed to adequately secure consumers' PII and, therefore, did not provide the full services that patient paid for. Patients now must monitor their personal, immutable PII for the rest of their lives.

112. If Plaintiffs and Class members would have known that Change Healthcare employed inadequate data security safeguards, they would not have agreed to providing Defendants with PII.

113. As a direct and proximate result of Change Healthcare's conduct, Plaintiffs and Class members have suffered the various types of damages alleged herein.

114. Class members have no adequate remedy at law. Change Healthcare continues to retain Class members' PII, and similar data security practices and vendors while exposing the PII to a risk of future data breaches in Defendants' possession.

115. Change Healthcare should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class members, proceeds that they unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiffs and Class members overpaid.

COUNT VI
Violation of the Minnesota Consumer Protection Statute on Deceptive Trade Practices Section 325d.44 and Data Warehouses Section 325E.61 Subdivision 1
(On Behalf of the Nationwide Class)

116. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully set forth herein.

117. The consumer protection statute Minn. R. 325D.44 describes a deceptive trade practice as when in course of business the person "(1) passes off goods or services as those of another;" or "(3) causes likelihood of confusion or of misunderstanding as to affiliation, connection, or association with, or certification by, another;" or "(7) represents that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another."

118. Change Healthcare represented itself as an expert in providing healthcare services compliant with particular industry standards relating to both healthcare IT and cybersecurity. However, once a common ransomware attack fractured Change Healthcare's systems, Change Healthcare hired additional outside cybersecurity firm aid.

119. The consumer protection statute Minn. R. 325E.61 subd. 1 defines "personal information" to inclusive of social security number, driver's license number, and credit card number.

120. Minn. R. 325E.61 subd. 1 also states:

> "The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in paragraph (c), or with any measures necessary to determine the scope of the breach, identify the individuals affected, and restore the reasonable integrity of the data system."

121. Change Healthcare violated disclosure in the most expedient time possible when its initial breach occurred in September 2020, but they did not notify Plaintiff's healthcare provider until January 2021.

122. Plaintiffs and Class members are also entitled to injunctive relief and an award of their attorney's fees and costs pursuant to this statute.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all others similarly situated, respectfully request the following relief:

(a) An Order certifying this case as a class action;

(b) An Order appointing Plaintiff as class representative;

(c) An Order appointing the undersigned counsel as class counsel;

(d) An award of compensatory damages to Plaintiff, money for significant and reasonable identity protection services, statutory damages, treble damages, and damages;

(e) Injunctive relief requiring Defendants to, *e.g.*: (i) strengthen and adequately fund their data security systems and monitoring procedures; (ii) submit to future independent annual audits of those systems and monitoring procedures; (iii) implement encryption of sensitive PII in all databases for all clients; and (iii) immediately provide free credit monitoring to all Class members;

(f) An Order for Defendants to pay equitable relief, in the form of disgorgement and restitution, and injunctive relief as may be appropriate;

(g) An Order for Defendants to pay both pre- and post-judgment interest on any amounts awarded; and

(h) An award of Plaintiff's attorneys' fees and litigation costs; and

(i) Such other and further relief as this Court may deem just and proper.

Dated: March 5, 2024

Respectfully submitted,

By: */s/David A. Goodwin*
Daniel E. Gustafson (#202241)
David A. Goodwin (#0386715)

Joe E. Nelson (#0402378)
GUSTAFSON GLUEK PLLC
Canadian Pacific Plaza
120 South Sixth Street, Suite 2600
Minneapolis, MN 55402
Tel: (612) 333-8844
dgustafson@gustafsongluek.com
dgoodwin@gustafsongluek.com
jnelson@gustafsongluek.com

Nicholas A. Migliaccio *
Jason S. Rathod *
MIGLICACCIO & RATHOD LLP
412 H St NE, Suite 302
Washington DC 20002
Telephone (202) 470-3520
nmigliaccio@classlawdc.com
jrathod@classlawdc.com

Attorneys for Plaintiff and Putative Class
**Pro Hac Vice Forthcoming*