UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MINNESOTA

AGIUS PSYCHOLOGICAL SERVICES, LLC; AUTHENTIC LIVING PSYCHOTHERAPY LLC; BALANCE FITNESS FOR LIFE, LLC; BALANCED LIFE COUNSELING SOLUTIONS, LLC D/B/A CARRIE LEAF THERAPY, LLC; BEGINNINGS AND BEYOND COUNSELING D/B/A PLAY THERAPY MINNESOTA; BELLO THERAPY; BRENT C. GARRARD COUNSELING, LLC; CEPD PSYCHOLOGICAL SERVICES; CROM REHABILITATION, LLC D/B/A ELATION PHYSICAL THERAPY; DOV WILLS, PLLC; DR. WARREN H. JOHNSON PC; DREW FISHER COUNSELING SERVICES, LLC; EAST PENN RHEUMATOLOGY; FRANK P. MAGGIACOMO, D.O., INC./MOC; GARRARD THERAPEUTIC PARTNERS, LLC; HEALTHFIRST FAMILY CARE CENTER, INC.; HOPE AND HARMONY COUNSELING, LLC; KILLINGLY DENTAL CARE LLC; K. WADE FOSTER, M.D., P.A., D/B/A FLORIDA DERMATOLOGY AND SKIN CARE CANCER CENTERS; KOKA CARDIOLOGY; KRISTIN PARKER, LMFT; LAURA COTTON LICSW; LDK COUNSELING, LLC; LISA RIPPERTON, LCSW, LCAS; MAGNOLIA MEDICAL CLINIC, P.A.; MELISSA MOREHOUSE LICSW LLC; M.P. COUNSELING SERVICES, PLLC; THE NATIONAL COMMUNITY PHARMACISTS ASSOCIATION; NORTH SHORE PHYSICAL THERAPY BELLAIRE, LLC; NORTHERN VERMONT DERMATOLOGY, PLC; SHAMYNDS HEALING CENTER, PC; SHEPARD HEALTH LLC; SOUTHEAST KANSAS EYE CARE ASSOCIATES, PA; SPACE COAST FOOT AND ANKLE CENTER, LLC; STRONG ROOTS THERAPY LLC; SUMMIT PSYCHIATRIC SERVICES, LLC; TELEBEHAVIORALHEALTH.US;

Case No.: 0:24-cv-02804

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

TRANSFORMATIVE INTIMACY LLC; TWIN CITIES COUNSELING LLC; and WIEMER FAMILY PODIATRY LLC, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

CHANGE HEALTHCARE INC., OPTUM, INC.; and UNITEDHEALTH GROUP INCORPORATED,

Defendants.

TABLE OF CONTENTS

Plaintiffs Agius Psychological Services, LLC ("Agius"), Authentic Living Psychotherapy LLC ("Authentic Living"), Balance Fitness for Life, LLC ("Balance Fitness"), Balanced Life Counseling Solutions, LLC d/b/a Carrie Leaf Therapy, LLC ("Carrie Leaf Therapy"), Beginnings and Beyond Counseling d/b/a Play Therapy Minnesota ("Beginnings"); Bello Therapy ("Bello"), Brent C. Garrard Counseling, LLC ("Garrard Counseling"), CEPD Psychological Services ("CEPD"), Crom Rehabilitation LLC d/b/a Elation Physical Therapy ("Elation PT"), Dov Wills, PLLC ("Wills"), Dr. Warren H. Johnson PC ("Johnson"), Drew Fisher Counseling Services, LLC ("Fisher"); East Penn Rheumatology ("East Penn"), Frank P. Maggiacomo, D.O., Inc./MOC ("Maggiacomo"), Garrard Therapeutic Partners, LLC ("Garrard Therapeutic"), HealthFirst Family Care Center, Inc. ("HealthFirst"), Hope and Harmony Counseling, LLC ("Hope"), Killingly Dental Care LLC ("Killingly"), K. Wade Foster, M.D., P.A., d/b/a Florida Dermatology and Skin Cancer Centers ("Florida Dermatology"), Koka Cardiology ("Koka"), Kristin Parker, LMFT ("Parker"), Laura Cotton LICSW ("Cotton"), LDK Counseling, LLC ("LDK"), Lisa Ripperton, LCSW, LCAS ("Ripperton"), Magnolia Medical Clinic, P.A. ("Magnolia"), Melissa Morehouse LICSW LLC ("Morehouse"), M.P. Counseling Services, PLLC ("M.P. Counseling"), North Shore Physical Therapy Bellaire, LLC ("NSPT"), Northern Vermont Dermatology, PLC ("NVD"), ShaMynds Healing Center, PC ("ShaMynds"), Shepard Health LLC ("Shepard Health"), Southeast Kansas Eye Care Associates, PA ("Southeast Eye Care"), Space Coast Foot and Ankle Center, LLC ("Space Coast"), Strong Roots Therapy LLC ("Strong Roots"), Summit Psychiatric Services, LLC ("Summit"), TelebehavioralHealth.US ("TelebehavioralHealth"),

Transformative Intimacy LLC ("Transformative"), Twin Cities Counseling LLC ("Twin Cities"), and Wiemer Family Podiatry LLC ("Wiemer") (collectively, "Provider Plaintiffs"), and the National Community Pharmacists Association ("NCPA," and together with Provider Plaintiffs, "Plaintiffs"), through their undersigned counsel, bring this class action complaint against Defendants UnitedHealth Group Incorporated ("UHG"), Optum, Inc. ("Optum"), and Change Healthcare Inc. ("Change," and together with UHG and Optum, "Defendants"), on behalf of themselves and all others similarly situated. Plaintiffs make the following allegations:

PRELIMINARY STATEMENT

1. "An urgent care chain in Ohio may be forced to stop paying rent and other bills to cover salaries. In Florida, a cancer center is racing to find money for chemotherapy drugs to avoid delaying critical treatments for its patients. And in Pennsylvania, a primary care doctor is slashing expenses and pooling all of her cash — including her personal bank stash — in the hopes of staying afloat for the next two months."[1] This was (and still is) the reality for many healthcare providers as a result of Defendants' response following what might be the most consequential data breach in history.

2. Defendants confirmed that a ransomware group accessed Change's servers and seized 6 terabytes of critical confidential and highly sensitive information, resulting in network outages that have already impacted millions of patients and physicians across the

[1] Reed Abelson & Julie Creswell, *Cyberattack Paralyzes the Largest U.S. Healthcare Payment System*, NYTIMES (Mar. 7, 2024), https://www.nytimes.com/2024/03/05/health/cyberattack-healthcare-cash.html.

country. On February 21, 2024, Defendants disclosed that Change was the subject of this massive data breach whereby hackers known as "ALPHV/Blackcat" ("Blackcat") gained unauthorized access to its unprotected network using an employee's compromised credentials (the "Data Breach").

3. Blackcat is a notable cybergroup that infiltrates healthcare institutions' internal servers through vulnerabilities in their networks. The group uses "ransomware to identify and attack 'high-value victim institutions[.]'"[2] According to the Department of Justice, Blackcat typically steals victims' data and encrypts the institution's data, networks, and servers, blocking the institution from accessing them. The group then demands the institution pay a ransom in exchange for the keys to decrypt the institution's network and servers. In exchange for ransom, Blackcat also offers a promise that it will not publish the institution's data to Blackcat's site on the Dark Web. Still, even when ransoms are paid, stolen data often ends up on the Dark Web. Blackcat has emerged as the second most prolific ransomware-as-a-service variant in the world.[3]

4. Blackcat also encrypted portions of Change's network, rendering them unusable. Change has still not fully recovered from this encryption.

---

[2] James Farrell, *Change Healthcare Blames 'Blackcat' Group for Cyber Attack That Disrupted Pharmacies and Health Systems*, FORBES (Feb. 29, 2024, 1:18 PM), https://www.forbes.com/sites/jamesfarrell/2024/02/29/change-healthcare-blames-blackcat-group-for-cyber-attack-that-disrupted-pharmacies-and-health-systems/?sh=589769fc1c4d.

[3] *Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant*, DOJ (Dec. 19, 2023), https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant.

5. Change confirmed that Blackcat accessed, copied, and exfiltrated highly sensitive information stored on Change's servers for millions of individuals, including Social Security numbers, driver's licenses, state ID numbers, passport numbers, health insurance information (such as primary, secondary or other health plans/policies, insurance companies, member/group ID numbers, and Medicaid-Medicare-government payor ID numbers), health information (such as medical record numbers, providers, diagnoses, medicines, test results, images, care and treatment), and/or billing, claims and payment information (such as claim numbers, account numbers, billing codes, payment cards, financial and banking information, payments made, and balance due) ("PII and PHI").[4]

6. The fallout from this Data Breach has wreaked havoc on the healthcare industry. As a subsidiary of one of the largest healthcare insurers, Change processes 15 billion transactions annually, "touching one in three U.S. patient records."[5] But to stop the cybersecurity wound from bleeding further, Defendants decided to take certain Change systems offline. One of these systems is the Change Healthcare platform ("Change Platform"). This platform provides, among other things, a claims processing service and a revenue and payment cycle management service that connects payers, providers, and

[4] *HIPAA WEBSITE SUBSTITUTE NOTICE*, CHANGE HEALTHCARE, https://www.changehealthcare.com/hipaa-substitute-notice?udm=14 (last visited July 18, 2024).

[5] Nicole Sganga & Andres Triay, *Cyberattack on UnitedHealth still impacting prescription access: "These are threats to life,"* CBS NEWS (Feb. 29, 2024, 9:00 PM), https://www.cbsnews.com/news/unitedhealth-cyberattack-change-healthcare-prescription-access-still-impacted/.

patients within the U.S. healthcare system.[6] The Change Platform is widely used among practitioners.

7. Reliance on Defendants' Change Platform has created a single point of failure in the U.S. health system. Without Defendants' Change Platform, the healthcare industry is immobilized. Patients were stuck in prescription purgatory without access to their vital medications. This is especially disruptive to elderly patients who have a fixed income and cannot afford medications without insurance, as well as individuals with chronic illnesses who face life-threatening symptoms without their medication. Defendants' network outage of the Change Platform jeopardized the health of millions of Americans.

8. Patients are not the only victims of the Data Breach. The ripple effect of the Data Breach is also hampering healthcare providers' practices. According to John Riggi, national advisor for cybersecurity and risk at the American Hospital Association, "[T]his cyberattack has affected every hospital in the country one way or another."[7] Many providers are still having trouble verifying patient eligibility and coverage, filing claims, and billing patients.[8] This leaves small and mid-sized practices especially vulnerable

---

[6] *Revenue Cycle Management*, CHANGE HEALTHCARE, https://www.changehealthcare.com/revenue-cycle-management (last visited July 16, 2024).

[7] Nicole Sganga & Andres Triay, *Cyberattack on UnitedHealth still impacting prescription access: "These are threats to life,"* CBS NEWS (Feb. 29, 2024, 9:00 PM), https://www.cbsnews.com/news/unitedhealth-cyberattack-change-healthcare-prescription-access-still-impacted/.

[8] Associated Press, *Minnetonka Based United Healthcare Hacked*, KNSI (Feb. 29, 2024, 5:46 PM), https://knsiradio.com/2024/02/29/minnetonka-based-united-healthcare-hacked/.

without normal cash flow to sustain operations. For over four months (and counting), these healthcare practices have received little, if any, reimbursement from insurers for patient visits. Without complete reimbursement, small and mid-sized practices cannot afford employee payroll, rent/mortgage, and medical supplies. This Data Breach has handicapped healthcare providers.

9. Exacerbating this crisis, Defendants have not provided adequate guidance to healthcare providers. Healthcare providers must notify their patients that their personally identifiable information ("PII") and PHI may have been compromised by the Data Breach. And, under certain conditions, they must report this breach to the federal government. However, Defendants have not provided adequate accounts about the Data Breach that would allow healthcare providers to satisfy their obligations. While at a Senate hearing, the CEO of Change's parent company, UHG, vowed to take responsibility for notifying patients about their stolen personal data; however, it took Defendants more than four months to start disseminating notice, which remains largely ongoing as of the time of this filing.[9] Without Defendants' guidance and commitment, healthcare providers are in a state of uncertainty.

10. Born of Defendants' carelessness, healthcare providers alike are feeling and will continue to feel the effects of the network outage for some time. Initially, UHG's Chief

[9] *HIPAA Website Substitute Notice*, Change Healthcare, https://www.changehealthcare.com/hipaa-substitute-notice?udm=14 (last visited July 16, 2024) (noting that the mailing process "is expected to begin in late July).

Operating Officer, Dirk McMahon, suggested that the outage could last weeks.[10] But Defendants' March 27, 2024 announcement that Change's network was back online noted that it was still not completely functional:

> [O]ur priority is to continue the flow of claims and build on functionality to support all your needs. We also continue to facilitate increased connectivity with payers, trading partners and submitters. The most important thing to get claims flowing at pre-incident levels is having a critical mass of payer connectivity established. Throughout the reactivation of these provider customer groups, we will continue to add additional payer connectivity to close any remaining gaps.[11]

11. The claims filings and payment processing functionality of the Change Platform is still not 100% of pre-data breach levels.

12. Defendants' indefinite delay has pushed many healthcare providers to the brink of closure (if not forced them to close altogether). To try to avoid this looming result, healthcare providers have incurred extra costs and switched to different healthcare software companies to assist with claim submission and revenue and payment management. Once again, this workaround hurts small and mid-sized practices the most. Not only were these practices weeks, if not months, behind on receiving payment, but they had to pay for another service with their remaining funds and learn an entirely new system all the while continuing to treat patients. Some providers had their claims outright rejected.

---

[10] Brittany Trang, *Change Healthcare cyberattack outage could persist for weeks, UnitedHealth Group executive suggests*, STAT (Feb. 29, 2024), https://www.statnews.com/2024/02/29/change-healthcare-cyber-attack-outage-will-last-for-weeks/.

[11] *Information on the Change Healthcare Cyber Response*, UNITEDHEALTH GROUP (Mar. 27, 2024), https://www.unitedhealthgroup.com/changehealthcarecyberresponse?zbrandid=3118.

13. Despite the disruption in Change's services and Defendants' failure to connect with healthcare providers, Defendants still manage to collect payment from healthcare practices.

14. Defendants are responsible for the Data Breach because they failed to implement reasonable security procedures and practices and failed to disclose material facts surrounding their deficient security protocols. Defendants admitted that Blackcat entered their externally facing server that was not protected with multifactor authentication (MFA). As Senator Wyden exclaimed during the Senate hearing, "this hack could have been stopped with cybersecurity 101."[12]

15. Responding to the Data Breach, Defendants claimed to have chosen to take systems offline to stop hackers from seizing more data than the 6 terabytes already taken. Defendants' decision caused this network outage that has severely impacted not only patients but healthcare practices and providers who rely on the Change Platform for processing claims and payment. As a result of Defendants' actions, Plaintiffs and Class members did not receive the benefit of their bargain with Defendants and are not receiving the services that they have paid for. Furthermore, Plaintiffs and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and have incurred extra costs from

[12] Pietje Kobus, *UnitedHealth CEO Testifies on Cyberattack Before Senate*, HEALTHCARE INNOVATION (May 2, 2024), https://www.hcinnovationgroup.com/cybersecurity/news/55036427/unitedhealth-ceo-testifies-on-cyberattack-before-senate.

switching to another healthcare payment software. And because Defendants do not have adequate redundancies, these consequences continue to harm Plaintiffs and Class members.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. There are more than 100 putative class members and at least some members of the proposed Class have a different citizenship from Defendants. This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367 because all claims alleged herein form part of the same case or controversy.

17. This Court may exercise jurisdiction over Defendants because they maintain their principal place of business in Minnesota, are registered to conduct business in Minnesota; have sufficient minimum contacts in Minnesota; and/or, intentionally avail themselves of the markets within Minnesota through the promotion, sale, and marketing of their services, thus rendering the exercise of jurisdiction by this Court proper and necessary.

18. Venue is proper in this District under 28 U.S.C. § 1391 because Defendants Optum and UHG reside in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District. In addition, the Judicial Panel on Multidistrict Litigation on June 7, 2024, issued an order centralizing litigation arising out of the Change Data Breach in this District.

NAMED PLAINTIFFS

19. The Provider Plaintiffs identified below bring this action on behalf of themselves and those similarly situated. Provider Plaintiffs are healthcare providers whose business operations were disrupted when Change disconnected the Change Platform from the network. Similarly, as alleged in greater detail below, NCPA represents the interests of more than 19,000 independent pharmacies nationwide ("NCPA Members").

20. Provider Plaintiffs and NCPA Members use and rely on the Change Platform to facilitate processing of insurance claims for approval and payment. In addition to payment, when claims are successfully processed, Provider Plaintiffs also receive an electronic remittance advice ("ERA") that summarizes the claim, the amount the insurance company will pay, and the amount the provider will write off. Along with lack of full payment from Defendants (if any payment at all), Provider Plaintiffs have not received ERAs, and thus are not informed as to what amounts the insurance company will cover. Provider Plaintiffs end up eating these costs without Defendants' functioning Change Platform. It was foreseeable that Defendants' substandard network security would lead to a data breach causing Change to disconnect its operations from the network, including the Change Platform. Had Defendants disclosed that their network security was not compliant with industry standards, Provider Plaintiffs and NCPA Members would have taken that into account when making their decisions about the most appropriate clearinghouse to process their claims. In particular, they would have engaged a competing clearinghouse for their services.

I. PLAINTIFF NCPA

21. Plaintiff NCPA maintains its principal place of business in Alexandria, Virginia. It was founded in 1898 and represents the interests of NCPA Members, which are the owners, managers, and employees of more than 19,400 independent community pharmacies. Almost half of all community pharmacies provide long-term care services and play a critical role in ensuring patients have immediate access to medications in both community and long-term care (LTC) settings. Together, NCPA Members represent a $94 billion healthcare marketplace, employ 230,000 individuals, and provide an expanding set of healthcare services to millions of patients every day. NCPA Members are small business owners who are among America's most accessible healthcare providers.

22. NCPA brings this action on behalf of all NCPA Members who are similarly situated with Provider Plaintiffs in that they use and rely on Defendants' services and the Change Platform in the daily operation of their businesses; therefore, as a result, NCPA Members have experienced immense business disruption and harm as a direct result of Defendants' substandard data security measures and the resulting data breach.

23. NCPA has standing to bring the instant lawsuit on behalf of NCPA Members because:

(a) NCPA Members have standing—as pharmacists directly impacted by the Change disruption—to sue Defendants in their own right for damages they have suffered as a result of Defendants' substandard data security measures;

(b) the interests NCPA seeks to protect in bringing these claims (i.e., seeking redress for the business disruption and attendant damages NCPA Members

have experienced as a result of Change's substandard data security measures) are germane to NCPA's purpose, which is to "protect[] and promote[] the interests of independent pharmacists whose current and future success is vital to their patients, their communities, and the entire health care system"[13]; and

(c) the claims NCPA asserts and the relief it seeks do not require the participation of individual NCPA Members in this lawsuit.

II. CALIFORNIA

A. Plaintiff Kristin Parker, LMFT

24. Plaintiff Kristin Parker, LMFT is a sole proprietorship with a residence in Placentia, California.

25. Plaintiff Parker relies on the Change Platform to provide, among other features, revenue and payment cycle management services.

26. Change Platform processes most of Plaintiff Parker's medical insurance claims and sends them to insurance companies for evaluation and payment. Once the claims are approved by the insurance company, Plaintiff Parker receives payment.

27. Put simply, without a functioning Change Platform, Plaintiff Parker does not get paid for her provision of medical services.

28. Because of Defendants' substandard data security measures, Defendants experienced the Data Breach. Defendants then chose to disconnect the Change Platform from the network.

[13] https://ncpa.org/about

29. As a result of this disconnection, Plaintiff Parker received delayed payments for the medical insurance claims she submitted or has had medical claims outright rejected by insurers.

30. As a result of Defendants' actions, Plaintiff Parker and Class members did not receive from Defendants the services that they have paid and/or bargained for, whether directly or indirectly with Defendants. In addition, Plaintiff Parker and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and/or have incurred extra costs from switching to another healthcare payment software. Furthermore, Plaintiff Parker spent significant time and resources, including, but not limited to, investigating the network outage, physically submitting medical claims, and/or applying for lines of credit as a result of the Change Platform and as a result of its loss/delay of income.

B. Plaintiff ShaMynds Healing Center, PC

31. Plaintiff ShaMynds Healing Center, PC is a California professional corporation with its principal place of business in Sacramento, California.

32. Plaintiff ShaMynds relies on the Change Platform to provide, among other features, revenue and payment cycle management services.

33. The Change Platform processes most of Plaintiff ShaMynds's medical insurance claims and sends them to insurance companies for evaluation and payment. Once the claims are approved by the insurance company, Plaintiff ShaMynds receives payment.

34. Put simply, without a functioning Change Platform, Plaintiff ShaMynds does not get paid for its provision of medical services.

35. Because of Defendants' substandard data security measures, Defendants experienced the Data Breach. Defendants then chose to disconnect the Change Platform from the network.

36. As a result of this disconnection, Plaintiff ShaMynds has not received full payment for the medical insurance claims it submitted or has had medical claims outright rejected by insurers. The practice is missing a significant amount in payment without any knowledge about if or when payment will be received.

37. As a result of Defendants' actions, Plaintiff ShaMynds and Class members did not receive from Defendants the services that they have paid and/or bargained for, whether directly or indirectly with Defendants. In addition, Plaintiff ShaMynds and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and/or have incurred extra costs from switching to another healthcare payment software. Furthermore, Plaintiff ShaMynds spent significant time and resources, including, but not limited to, investigating the network outage, physically submitting medical claims, and/or applying for lines of credit as a result of the Change Platform and as a result of its loss/delay of income.

III. CONNECTICUT

A. Killingly Dental Care LLC

38. Plaintiff Killingly Dental Care LLC ("Killingly") is a Connecticut limited liability company with its principal place of business in Dayville, Connecticut whose sole member is a Massachusetts citizen.

39. Plaintiff Killingly relies on the Change Platform to provide, among other features, revenue and payment cycle management services.

40. The Change Platform processes most of Plaintiff Killingly's dental insurance claims and sends them to insurance companies for evaluation and payment. Once the claims are approved by the insurance company, Plaintiff Killingly receives payment.

41. Put simply, without a functioning Change Platform, Plaintiff Killingly does not get paid for its provision of dental services.

42. Because of Defendants' substandard data security measures, Defendants experienced the Data Breach. Defendants then chose to disconnect its Change Platform from the network.

43. As a result of this disconnection, Plaintiff Killingly has not received full payment for the dental insurance claims it submitted or has had dental claims outright rejected by insurers. The practice is missing a significant amount in payment without any knowledge about if or when payment will be received.

44. As a result of Defendants' actions, Plaintiff Killingly and Class members did not receive from Defendants the services that they have paid and/or bargained for, whether directly or indirectly with Defendants. In addition, Plaintiff Killingly and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and/or have incurred extra costs from switching to another healthcare payment software. Furthermore, Plaintiff Killingly spent significant time and resources, including, but not limited to, investigating

the network outage, physically submitting dental insurance claims, and/or applying for lines of credit as a result of the Change Platform and as a result of its loss/delay of income.

IV. FLORIDA

A. Plaintiff K. Wade Foster, M.D., P.A., d/b/a Florida Dermatology and Skin Cancer Centers

45. Plaintiff K. Wade Foster, M.D., P.A., d/b/a Florida Dermatology and Skin Cancer Centers ("Florida Dermatology") is a Florida Professional Association with its principal place of business in Davenport, Florida.

46. Plaintiff Florida Dermatology has 15 offices spread throughout central Florida and employs 6 physicians, 11 non-physician medical professionals, and a staff of 119.

47. Plaintiff Florida Dermatology relies on the Change Platform to provide, among other features, revenue and payment cycle management services.

48. The Change Platform processes most of Florida Dermatology's insurance claims and sends them to insurance companies for evaluation and payment. Once the claims are approved by the insurance company, Plaintiff Florida Dermatology receives payment. Put simply, without a functioning Change Platform, Plaintiff Florida Dermatology does not get paid for its provision of medical services.

49. Because of Defendants' substandard data security measures, Defendants experienced the Data Breach. Defendants then chose to disconnect the Change Platform from the network.

50. As a result of this disconnection, Plaintiff Florida Dermatology has not received full payment for the medical insurance claims it submitted or has had medical claims outright rejected by insurers.

51. As a result of Defendants' actions, Plaintiff Florida Dermatology and Class members did not receive from Defendants the services that they have paid and/or bargained for, whether directly or indirectly with Defendants. In addition, Plaintiff Florida Dermatology and Class members have not received payments for their healthcare services or have received late payments, depriving them of the time-value of money and loss of interest and/or have incurred extra costs from switching to another healthcare payment software. Furthermore, Plaintiff Florida Dermatology spent significant time and resources, including, but not limited to, investigating the network outage, physically submitting medical claims, and/or investigating lines of credit as a result of the Change Platform and as a result of its loss/delay of income.

B. Plaintiff Magnolia Medical Clinic, P.A.

52. Plaintiff Magnolia Medical Clinic, P.A. is a Florida corporation with its principal place of business in Fort Walton Beach, Florida.

53. Plaintiff Magnolia relies on the Change Platform to provide, among other features, revenue and payment cycle management services.

54. The Change Platform processes most of Plaintiff Magnolia's medical insurance claims and sends them to insurance companies for evaluation and payment. Once the claims are approved by the insurance company, Plaintiff Magnolia receives payment.

55. Put simply, without a functioning Change Platform, Plaintiff Magnolia does not get paid for its provision of medical services.

56. Because of Defendants' substandard data security measures, Defendants experienced the Data Breach. Defendants then chose to disconnect the Change Platform from the network.

57. As a result of this disconnection, Plaintiff Magnolia has not received full payment for the medical insurance claims it submitted or has had medical claims outright rejected by insurers. The practice is missing a significant amount in payment without any knowledge about if or when payment will be received.

58. As a result of Defendants' actions, Plaintiff Magnolia and Class members did not receive from Defendants the services that they have paid and/or bargained for, whether directly or indirectly with Defendants. In addition, Plaintiff Magnolia and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and/or have incurred extra costs from switching to another healthcare payment software. Furthermore, Plaintiff Magnolia spent significant time and resources, including, but not limited to, investigating the network outage, physically submitting medical claims, and/or applying for lines of credit as a result of the Change Platform and as a result of its loss/delay of income.

C. Plaintiff Space Coast Foot and Ankle Center, LLC

59. Plaintiff Space Coast Foot and Ankle Center, LLC is a Florida limited liability company with its principal place of business in Melbourne, Florida, and whose sole member is a Florida citizen.

60. Plaintiff Space Coast relies on the Change Platform to provide, among other features, revenue and payment cycle management services.

61. The Change Platform processes most of Plaintiff Space Coast's medical insurance claims and sends them to insurance companies for evaluation and payment. Once the claims are approved by the insurance company, Plaintiff Space Coast receives payment.

62. Put simply, without a functioning Change Platform, Plaintiff Space Coast does not get paid for its provision of medical services.

63. Because of Defendants' substandard data security measures, Defendants experienced the Data Breach. Defendants then chose to disconnect the Change Platform from the network.

64. As a result of this disconnection, Plaintiff Space Coast has not received full payment for the medical insurance claims it submitted or has had medical claims outright rejected by insurers. The practice is missing a significant amount in payment without any knowledge about if or when payment will be received.

65. As a result of Defendants' actions, Plaintiff Space Coast and Class members did not receive from Defendants the services that they have paid and/or bargained for, whether directly or indirectly with Defendants. In addition, Plaintiff Space Coast and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and/or have incurred extra costs from switching to another healthcare payment software. Furthermore, Plaintiff Space Coast spent significant time and resources, including but not limited to,

investigating the network outage and physically submitting medical claims as a result of the Change Platform and as a result of its loss/delay of income.

V. GEORGIA

A. Plaintiff Shepard Health LLC

66. Plaintiff Shepard Health LLC is a Georgia limited liability company with its principal place of business in Sandy Springs, Georgia, and whose sole members are Georgia citizens.

67. Plaintiff Shepard Health relies on the Change Platform to provide, among other features, revenue and payment cycle management services.

68. The Change Platform processes most of Plaintiff Shepard Health's medical insurance claims and sends them to insurance companies for evaluation and payment. Once the claims are approved by the insurance company, Plaintiff Shepard Health receives payment.

69. Put simply, without a functioning Change Platform, Plaintiff Shepard Health does not get paid for its provision of medical services.

70. Because of Defendants' substandard data security measures, Defendants experienced the Data Breach. Defendants then chose to disconnect the Change Platform from the network.

71. As a result of this disconnection, Plaintiff Shepard Health has not received full payment for the medical insurance claims it submitted or has had medical claims outright rejected by insurers. The practice is missing a significant amount in payment without any knowledge about if or when payment will be received.

72. As a result of Defendants' actions, Plaintiff Shepard Health and Class members did not receive from Defendants services that they have paid and/or bargained for, whether directly or indirectly with Defendants. In addition, Plaintiff Shepard Health and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and/or have incurred extra costs from switching to another healthcare payment software. Furthermore, Plaintiff Shepard Health spent significant time and resources, including, but not limited to, investigating the network outage, physically submitting medical claims, and/or applying for lines of credit as a result of the Change Platform and as a result of its loss/delay of income.

VI. ILLINOIS

A. Plaintiff Balance Fitness for Life, LLC

73. Plaintiff Balance Fitness is an Illinois limited liability company with its principal place of business in Chicago, Illinois.

74. Plaintiff Balance Fitness relies on the Change Platform to provide, among other features, revenue and payment cycle management services.

75. The Change Platform processes most of Plaintiff Balance Fitness's medical insurance claims and sends them to insurance companies for evaluation and payment. Once the claims are approved by the insurance company, Plaintiff Balance Fitness receives payment.

76. Put simply, without a functioning Change Platform, Plaintiff Balance Fitness does not get paid for its provision of medical services.

77. Because of Defendants' substandard data security measures, Defendants experienced the Data Breach. Defendants then chose to disconnect the Change Platform from the network.

78. As a result of this disconnection, Plaintiff Balance Fitness has not received full payment for the medical insurance claims it submitted or has had medical claims outright rejected by insurers. The practice is missing a significant amount in payment without any knowledge about if or when payment will be received.

79. As a result of Defendants' actions, Plaintiff Balance Fitness and Class members did not receive from Defendants services that they have paid and/or bargained for, whether directly or indirectly with Defendants. In addition, Plaintiff Balance Fitness and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and/or have incurred extra costs from switching to another healthcare payment software. Furthermore, Plaintiff Balance Fitness spent significant time and resources, including, but not limited to, investigating the network outage and physically submitting and mailing medical claims as a result of the Change Platform and as a result of its loss/delay of income.

VII. IOWA

A. Plaintiff Balanced Life Counseling Solutions, LLC d/b/a Carrie Leaf Therapy, LLC

80. Plaintiff Carrie Leaf Therapy is an Iowa limited liability company with its principal place of business in West Des Moines, Iowa whose sole member is an Iowa citizen.

81. Plaintiff Carrie Leaf Therapy relies on the Change Platform to provide, among other features, revenue and payment cycle management services.

82. The Change Platform processes most of Plaintiff Carrie Leaf Therapy's medical insurance claims and sends them to insurance companies for evaluation and payment. Once the claims are approved by the insurance company, Plaintiff Carrie Leaf Therapy receives payment.

83. Put simply, without a functioning Change Platform, Plaintiff Carrie Leaf Therapy does not get paid for its provision of medical services.

84. Because of Defendants' substandard data security measures, Defendants experienced the Data Breach. Defendants then chose to disconnect the Change Platform from the network.

85. As a result of this disconnection, Plaintiff Carrie Leaf Therapy has not received full payment for the medical insurance claims it submitted or has had medical claims outright rejected by insurers. The practice is missing a significant amount in payment without any knowledge about if or when payment will be received.

86. As a result of Change's actions, Plaintiff Carrie Leaf Therapy and Class members did not receive from Defendants services that they have paid and/or bargained for, whether directly or indirectly with Defendants. In addition, Plaintiff Carrie Leaf Therapy and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and/or have incurred extra costs from switching to another healthcare payment software. Furthermore, Plaintiff Carrie Leaf Therapy has spent significant time and resources,

including, but not limited to, investigating the network outage, learning and transitioning to a new clearinghouse, and physically submitting and mailing medical claims as a result of the Change Platform and as a result of its loss/delay of income.

VIII. KANSAS

A. Plaintiff Southeast Kansas Eye Care Associates, P.A.

87. Plaintiff Southeast Kansas Eye Care Associates, P.A. is a Kansas professional association with its principal place of business in Coffeyville, Kansas.

88. Plaintiff Southeast Eye Care relies on the Change Platform to provide, among other features, revenue and payment cycle management services.

89. The Change Platform processes most of Plaintiff Southeast Eye Care's medical insurance claims and sends them to insurance companies for evaluation and payment. Once the claims are approved by the insurance company, Plaintiff Southeast Eye Care receives payment.

90. Put simply, without a functioning Change Platform, Plaintiff Southeast Eye Care does not get paid for its provision of medical services.

91. Because of Defendants' substandard data security measures, Defendants experienced the Data Breach. Defendants then chose to disconnect the Change Platform from the network.

92. As a result of this disconnection, Plaintiff Southeast Eye Care has not received full payment for the medical insurance claims it submitted or has had medical claims outright rejected by insurers. The practice is missing a significant amount in payment without any knowledge about if or when payment will be received.

93. As a result of Defendants' actions, Plaintiff Southeast Eye Care and Class members did not receive from Defendants services that they have paid and/or bargained for, whether directly or indirectly with Defendants. In addition, Plaintiff Southeast Eye Care and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and/or have incurred extra costs from switching to another healthcare payment software. Furthermore, Plaintiff Southeast Eye Care spent significant time and resources, including, but not limited to, investigating the network outage, physically submitting medical claims, and/or applying for lines of credit as a result of the Change Platform and as a result of its loss/delay of income.

IX. KENTUCKY

A. Plaintiff Brent C. Garrard Counseling, LLC at Garrard Therapeutic Partners, LLC

94. Plaintiff Brent C. Garrard Counseling, LLC is a Kentucky limited liability company with its principal place of business in Owensboro, Kentucky whose sole member is a Kentucky citizen.

95. Plaintiff Garrard Counseling relies on the Change Platform to provide, among other features, revenue and payment cycle management services.

96. The Change Platform processes most of Plaintiff Garrard Counseling's medical insurance claims and sends them to insurance companies for evaluation and payment. Once the claims are approved by the insurance company, Plaintiff Garrard Counseling receives payment.

97. Put simply, without a functioning Change Platform, Plaintiff Garrard Counseling does not get paid for its provision of medical services.

98. Because of Defendants' substandard data security measures, Defendants experienced the Data Breach. Defendants then chose to disconnect the Change Platform from the network.

99. As a result of this disconnection, Plaintiff Garrard Counseling has not received full payment for the medical insurance claims it submitted or has had medical claims outright rejected by insurers. The practice is missing a significant amount in payment without any knowledge about if or when payment will be received.

100. As a result of Defendants' actions, Plaintiff Garrard Counseling and Class members did not receive from Defendants services that they have paid and/or bargained for, whether directly or indirectly with Defendants. In addition, Plaintiff Garrard Counseling and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and/or have incurred extra costs from switching to another healthcare payment software. Furthermore, Plaintiff Garrard Counseling spent significant time and resources, including, but not limited to, investigating the network outage, physically submitting medical claims, and/or applying for lines of credit as a result of the Change Platform and as a result of its loss/delay of income.

B. Plaintiff Garrard Therapeutic Partners, LLC

101. Plaintiff Garrard Therapeutic Partners, LLC is a Kentucky limited liability company with its principal place of business in Owensboro, Kentucky whose sole member is a Kentucky citizen.

102. Plaintiff Garrard Therapeutic relies on the Change Platform to provide, among other features, revenue and payment cycle management services.

103. The Change Platform processes most of Plaintiff Garrard Therapeutic's medical insurance claims and sends them to insurance companies for evaluation and payment. Once the claims are approved by the insurance company, Plaintiff Garrard Therapeutic receives payment.

104. Put simply, without a functioning Change Platform, Plaintiff Garrard Therapeutic does not get paid for its provision of medical services.

105. Because of Defendants' substandard data security measures, Defendants experienced the Data Breach. Defendants then chose to disconnect the Change Platform from the network.

106. As a result of this disconnection, Plaintiff Garrard Therapeutic has not received full payment for the medical insurance claims it submitted or has had medical claims outright rejected by insurers. The practice is missing a significant amount in payment without any knowledge about if or when payment will be received.

107. As a result of Defendants' actions, Plaintiff Garrard Therapeutic and Class members did not receive from Defendants the services that they have paid and/or bargained for, whether directly or indirectly with Defendants. In addition, Plaintiff Garrard

Therapeutic and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and/or have incurred extra costs from switching to another healthcare payment software. Furthermore, Plaintiff Garrard Therapeutic spent significant time and resources, including, but not limited to, investigating the network outage, physically submitting medical claims, and/or applying for lines of credit as a result of the Change Platform and as a result of its loss/delay of income.

X. LOUISIANA

A. Plaintiff Dr. Warren H. Johnson PC

108. Plaintiff Dr. Warren H. Johnson is a sole proprietorship with a residence in New Orleans, Louisiana.

109. Plaintiff Dr. Johnson relies on the Change Platform to provide, among other features, revenue and payment cycle management services.

110. The Change Platform processes most of Plaintiff Dr. Johnson's medical insurance claims and sends them to insurance companies for evaluation and payment. Once the claims are approved by the insurance company, Plaintiff Dr. Johnson receives payment.

111. Put simply, without a functioning Change Platform, Plaintiff Dr. Johnson does not get paid for its provision of medical services.

112. Because of Defendants' substandard data security measures, Defendants experienced the Data Breach. Defendants then chose to disconnect the Change Platform from the network.

113. As a result of this disconnection, Plaintiff Dr. Johnson has not received full payment for the medical insurance claims it submitted or has had medical claims outright rejected by insurers. The practice is missing a significant amount in payment without any knowledge about if or when payment will be received.

114. As a result of Change's actions, Plaintiff Dr. Johnson and Class did not receive from Defendants the services that they have paid and/or bargained for, whether directly or indirectly with Defendants. In addition, Plaintiff Dr. Johnson and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and/or have incurred extra costs from switching to another healthcare payment software. Furthermore, Plaintiff Dr. Johnson spent significant time and resources, including, but not limited to, investigating the network outage, physically submitting medical claims, and applying for lines of credit as a result of the Change Platform and as a result of its loss/delay of income.

XI. MASSACHUSETTS

A. Plaintiff Bello Therapy

115. Plaintiff Bello Therapy is a sole proprietorship with a primary residence in Boston, Massachusetts.

116. Plaintiff Bello relies on the Change Platform to provide, among other features, revenue and payment cycle management services.

117. The Change Platform processes most of Plaintiff Bello's medical insurance claims and sends them to insurance companies for evaluation and payment. Once the claims are approved by the insurance company, Plaintiff Bello receives payment.

118. Put simply, without a functioning Change Platform, Plaintiff Bello does not get paid for its provision of medical services.

119. Because of Defendants' substandard data security measures, Defendants experienced the Data Breach. Defendants then chose to disconnect the Change Platform from the network.

120. As a result of this disconnection, Plaintiff Bello has not received full payment for the medical insurance claims it submitted or has had medical claims outright rejected by insurers.

121. As a result of Defendants' actions, Plaintiff Bello and Class members did not receive from Defendants the services that they have paid and/or bargained for, whether directly or indirectly with Defendants. In addition, Plaintiff Bello and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and/or have incurred extra costs from switching to another healthcare payment software. Furthermore, Plaintiff Bello spent significant time and resources, including, but not limited to, investigating the network outage, physically submitting medical claims, researching new claims processing platforms, and/or applying for lines of credit as a result of the Change Platform and as a result of its loss/delay of income.

B. Plaintiff Laura Cotton LICSW

122. Plaintiff Laura Cotton LICSW is a sole proprietorship with a primary residence in Malden, Massachusetts.

123. Plaintiff Cotton relies on the Change Platform to provide, among other features, revenue and payment cycle management services.

124. The Change Platform processes Plaintiff Cotton's medical insurance claims and sends them to insurance companies for evaluation and payment. Once the claims are approved by the insurance company, Plaintiff Cotton receives payment.

125. Put simply, without a functioning Change Platform, Plaintiff Cotton does not get paid for her provision of medical services.

126. Because of Defendants' substandard data security measures, Defendants experienced the Data Breach. Defendants then chose to disconnect the Change Platform from the network.

127. As a result of the Data Breach, Plaintiff Cotton received delayed payments for the medical insurances claims she submitted or has had medical claims outright rejected by insurers.

128. As a result of Change's actions, Plaintiff Cotton and Class members did not receive from Defendants the services that they have paid and/or bargained for, whether directly or indirectly with Defendants. In addition, Plaintiff Cotton and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and/or have incurred extra costs from switching to another healthcare payment software. Furthermore, Plaintiff Cotton spent significant time and resources, including, but not limited to, investigating the network outage and physically submitting medical claims as a result of the Change Platform and as a result of her loss/delay of income.

C. Plaintiff Melissa Morehouse LICSW LLC

129. Plaintiff Melissa Morehouse LICSW LLC is a Massachusetts limited liability company with its principal place of business in Beverly, Massachusetts, and whose sole member is a Massachusetts citizen.

130. Plaintiff Morehouse relies on the Change Platform to provide, among other features, revenue and payment cycle management services.

131. The Change Platform processes most of Plaintiff Morehouse's medical insurance claims and sends them to insurance companies for evaluation and payment. Once the claims are approved by the insurance company, Plaintiff Morehouse receives payment.

132. Put simply, without a functioning Change Platform, Plaintiff Morehouse does not get paid for its provision of medical services.

133. Because of Defendants' substandard data security measures, Defendants experienced the Data Breach. Defendants then chose to disconnect the Change Platform from the network.

134. As a result of this disconnection, Plaintiff Morehouse has not received full payment for the medical insurance claims it submitted or has had medical claims outright rejected by insurers.

135. As a result of Change's actions, Plaintiff Morehouse and Class members did not receive from Defendants the services that they have paid and/or bargained for, whether directly or indirectly with Defendants. In addition, Plaintiff Morehouse and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and/or have incurred extra

costs from switching to another healthcare payment software. Furthermore, Plaintiff Morehouse spent significant time and resources, including, but not limited to, investigating the network outage and physically submitting medical claims as a result of the Change Platform and as a result of its loss/delay of income.

D. Plaintiff Transformative Intimacy LLC

136. Plaintiff Transformative Intimacy LLC is a Massachusetts limited liability company with its principal place of business in Andover, Massachusetts, and whose sole member is a Massachusetts citizen.

137. Plaintiff Transformative relies on the Change Platform to provide, among other features, revenue and payment cycle management services.

138. The Change Platform processes most of Plaintiff Transformative's medical insurance claims and sends them to insurance companies for evaluation and payment. Once the claims are approved by the insurance company, Plaintiff Transformative receives payment.

139. Put simply, without a functioning Change Platform, Plaintiff Transformative does not get paid for its provision of medical services.

140. Because of Defendants' substandard data security measures, Defendants experienced the Data Breach. Defendants then chose to disconnect the Change Platform from the network.

141. As a result of this disconnection, Plaintiff Transformative has not received full payment for the medical insurance claims it submitted or has had medical claims

outright rejected by insurers. The practice is missing a significant amount in payment without any knowledge about if or when payment will be received.

142. As a result of Defendants' actions, Plaintiff Transformative and Class members did not receive from Defendants the services that they have paid and/or bargained for, whether directly or indirectly with Defendants. In addition, Plaintiff Transformative and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and/or have incurred extra costs from switching to another healthcare payment software. Furthermore, Plaintiff Transformative spent significant time and resources, including, but not limited to, investigating the network outage and physically submitting medical claims as a result of the Change Platform and as a result of its loss/delay of income.

XII. MICHIGAN

A. Plaintiff Agius Psychological Services, LLC

143. Plaintiff Agius Psychological Services, LLC is a Michigan limited liability company with its principal place of business in Fenton, Michigan, and whose sole member is a Michigan citizen.

144. Plaintiff Agius relies on the Change Platform to provide, among other features, revenue and payment cycle management services.

145. The Change Platform processes most of Plaintiff Agius's medical insurance claims and sends them to insurance companies for evaluation and payment. Once the claims are approved by the insurance company, Plaintiff Agius receives payment.

146. Put simply, without a functioning Change Platform, Plaintiff Agius does not get paid for its provision of medical services.

147. Because of Defendants' substandard data security measures, Defendants experienced the Data Breach. Defendants then chose to disconnect the Change Platform from the network.

148. As a result of this disconnection, Plaintiff Agius has not received full payment for the medical insurance claims it submitted or has had medical claims outright rejected by insurers. The practice is missing a significant amount in payment without any knowledge about if or when payment will be received.

149. As a result of Defendants' actions, Plaintiff Agius and Class members did not receive from Defendants the services that they have paid and/or bargained for, whether directly or indirectly with Defendants. In addition, Plaintiff Agius and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and/or have incurred extra costs from switching to another healthcare payment software. Furthermore, Plaintiff Agius spent significant time and resources, including, but not limited to, investigating the network outage and physically submitting medical claims as a result of the Change Platform and as a result of its loss/delay of income.

B. Plaintiff Authentic Living Psychotherapy LLC

150. Plaintiff Authentic Living Psychotherapy LLC is a Michigan limited liability corporation with a principal place of business in Detroit, Michigan, and practices in Michigan and Connecticut.

151. Plaintiff Authentic Living relies on the Change Platform to provide, among other features, revenue and payment cycle management services.

152. The Change Platform processes most of Plaintiff Authentic Living's medical insurance claims and sends them to insurance companies for evaluation and payment. Once the claims are approved by the insurance company, Plaintiff Authentic Living receives payment.

153. Put simply, without a functioning Change Platform, Plaintiff Authentic Living does not get paid for its provision of medical services.

154. Because of Defendants' substandard data security measures, Defendants experienced the Data Breach. Defendants then chose to disconnect the Change Platform from the network.

155. As a result of this disconnection, Plaintiff Authentic Living received delayed payments for the medical insurance claims it submitted or has had medical claims outright rejected by insurers.

156. As a result of Defendants' actions, Plaintiff Authentic Living and Class members did not receive from Defendants the services that they have paid and/or bargained for, whether directly or indirectly with Defendants. In addition, Plaintiff Authentic Living and Class members received late payments depriving them of the time-value of money and loss of interest and/or have incurred extra costs from switching to another healthcare payment software. Furthermore, Plaintiff Authentic Living spent significant time and resources, including, but not limited to, investigating the network outage and physically

submitting medical claims as a result of the Change Platform and as a result of its loss/delay of income.

C. Plaintiff North Shore Physical Therapy Bellaire, LLC

157. Plaintiff North Shore Physical Therapy Bellaire, LLC is a Michigan limited liability company with its principal place of business in Bellaire, Michigan whose sole member is a Michigan citizen.

158. Plaintiff NSPT relies on the Change Platform to provide, among other features, revenue and payment cycle management services.

159. The Change Platform processes most of Plaintiff NSPT's medical insurance claims and sends them to insurance companies for evaluation and payment. Once the claims are approved by the insurance company, Plaintiff NSPT receives payment.

160. Put simply, without a functioning Change Platform, Plaintiff NSPT does not get paid for its provision of medical services.

161. Because of Defendants' substandard data security measures, Defendants experienced the Data Breach. Defendants then chose to disconnect the Change Platform from the network.

162. As a result of this disconnection, Plaintiff NSPT has not received full payment for the medical insurance claims it submitted or has had medical claims outright rejected by insurers. The practice is missing a significant amount in payment without any knowledge about if or when payment will be received.

163. As a result of Defendants' actions, Plaintiff NSPT and Class members did not receive from Defendants the services that they have paid and/or bargained for, whether

directly or indirectly with Defendants. In addition, Plaintiff NSPT and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and/or have incurred extra costs from switching to another healthcare payment software. Furthermore, Plaintiff NSPT spent significant time and resources, including, but not limited to, investigating the network outage, physically submitting medical claims, and/or applying for lines of credit as a result of the Change Platform and as a result of its loss/delay of income.

D. Plaintiff Strong Roots Therapy LLC

164. Plaintiff Strong Roots Therapy LLC is a Michigan limited liability company with its principal place of business in Clay, Michigan whose sole member is a Michigan citizen.

165. Plaintiff Strong Roots relies on the Change Platform to provide, among other features, revenue and payment cycle management services.

166. The Change Platform processes most of Plaintiff Strong Roots' medical insurance claims and sends them to insurance companies for evaluation and payment. Once the claims are approved by the insurance company, Plaintiff Strong Roots receives payment.

167. Put simply, without a functioning Change Platform, Plaintiff Strong Roots does not get paid for its provision of medical services.

168. Because of Defendants' substandard data security measures, Defendants experienced the Data Breach. Defendants then chose to disconnect the Change Platform from the network.

169. As a result of this disconnection, Plaintiff Strong Roots has not received full payment for the medical insurance claims it submitted or has had medical claims outright rejected by insurers. The practice is missing a significant amount in payment without any knowledge about if or when payment will be received.

170. As a result of Defendants' actions, Plaintiff Strong Roots and Class members did not receive from Defendants the services that they have paid and/or bargained for, whether directly or indirectly with Defendants. In addition, Plaintiff Strong Roots and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and/or have incurred extra costs from switching to another healthcare payment software. Furthermore, Plaintiff Strong Roots spent significant time and resources, including, but not limited to, investigating the network outage, physically submitting medical claims, and/or applying for lines of credit as a result of the Change Platform and as a result of its loss/delay of income.

E. Plaintiff TelebehavioralHealth.US

171. Plaintiff TelebehavioralHealth.US ("TelebehavioralHealth") is a Michigan company with its principal place of business in Grand Rapids, Michigan.

172. Plaintiff TelebehavioralHealth relies on the Change Platform to provide, among other features, revenue and payment cycle management services.

173. The Change Platform processes most of Plaintiff TelebehavioralHealth's medical insurance claims and sends them to insurance companies for evaluation and

payment. Once the claims are approved by the insurance company, Plaintiff TelebehavioralHealth receives payment.

174. Put simply, without a functioning Change Platform, Plaintiff TelebehavioralHealth does not get paid for its provision of medical services.

175. Because of Defendants' substandard data security measures, Defendants experienced the Data Breach. Defendants then chose to disconnect the Change Platform from the network.

176. As a result of this disconnection, Plaintiff TelebehavioralHealth has not received full payment for the medical insurance claims it submitted or has had medical claims outright rejected by insurers. The practice is missing a significant amount in payment without any knowledge about if or when payment will be received.

177. As a result of Defendants' actions, Plaintiff TelebehavioralHealth and Class members did not receive from Defendants the services that they have paid and/or bargained for, whether directly or indirectly with Defendants. In addition, Plaintiff TelebehavioralHealth and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and/or have incurred extra costs from switching to another healthcare payment software. Furthermore, Plaintiff TelebehavioralHealth spent significant time and resources, including, but not limited to, investigating the network outage and physically submitting medical claims as a result of the Change Platform and as a result of its loss/delay of income.

XIII. MINNESOTA

A. Plaintiff Beginnings and Beyond Counseling d/b/a Play Therapy Minnesota

178. Plaintiff Beginnings and Beyond Counseling d/b/a Play Therapy is a Minnesota limited liability company with its principal place of business in Edina, Minnesota.

179. Plaintiff Beginnings relies on the Change Platform to provide, among other features, revenue and payment cycle management services.

180. The Change Platform processes Plaintiff Beginnings's medical insurance claims and sends them to insurance companies for evaluation and payment. Once the claims are approved by the insurance company, Plaintiff Beginnings receives payment.

181. Put simply, without a functioning Change Platform, Plaintiff Beginnings does not get paid for its provision of medical services.

182. Because of Defendants' substandard data security measures, Defendants experienced the Data Breach. Defendants then chose to disconnect the Change Platform from the network.

183. As a result of this disconnection, Plaintiff Beginnings has not received full payment for the medical insurance claims it submitted or has had medical claims outright rejected by insurers. The practice is missing a significant amount in payment without any knowledge about if or when payment will be received.

184. As a result of Defendants' actions, Plaintiff Beginnings and Class members did not receive from Defendants the services that they have paid and/or bargained for,

whether directly or indirectly with Defendants. In addition, Plaintiff Beginnings and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and/or have incurred extra costs from switching to another healthcare payment software. Furthermore, Plaintiff Beginnings spent significant time and resources, including, but not limited to, investigating the network outage and physically submitting medical claims as a result of the Change Platform and as a result of its loss/delay of income.

B. Plaintiff Twin Cities Counseling LLC

185. Plaintiff Twin Cities Counseling LLC is a Minnesota corporation with its principal place of business in Minneapolis, Minnesota.

186. Plaintiff Twin Cities relies on the Change Platform to provide, among other features, revenue and payment cycle management services.

187. The Change Platform processes most of Plaintiff Twin Cities' medical insurance claims and sends them to insurance companies for evaluation and payment. Once the claims are approved by the insurance company, Plaintiff Twin Cities receives payment.

188. Put simply, without a functioning Change Platform, Plaintiff Twin Cities does not get paid for its provision of medical services.

189. Because of Defendants' substandard data security measures, Defendants experienced the Data Breach. Defendants then chose to disconnect the Change Platform from the network.

190. As a result of this disconnection, Plaintiff Twin Cities has not received full payment for the medical insurance claims it submitted or has had medical claims outright

rejected by insurers. The practice is missing a significant amount in payment without any knowledge about if or when payment will be received.

191. As a result of Defendants' actions, Plaintiff Twin Cities and Class members did not receive from Defendants the services that they have paid and/or bargained for, whether directly or indirectly with Defendants. In addition, Plaintiff Twin Cities and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and/or have incurred extra costs from switching to another healthcare payment software. Furthermore, Plaintiff Twin Cities spent significant time and resources, including, but not limited to, investigating the network outage and physically submitting medical claims as a result of the Change Platform and as a result of its loss/delay of income.

XIV. MISSOURI

A. Plaintiff Drew Fisher Counseling Services, LLC

192. Plaintiff Drew Fisher Counseling Services, LLC is a Missouri limited liability company with its principal place of business in St. Joseph, Missouri whose sole member is a Missouri citizen.

193. Plaintiff Fisher Counseling relies on the Change Platform to provide, among other features, revenue and payment cycle management services.

194. The Change Platform processes most of Plaintiff Fisher Counseling's medical insurance claims and sends them to insurance companies for evaluation and payment. Once the claims are approved by the insurance company, Plaintiff Fisher Counseling receives payment.

195. Put simply, without a functioning Change Platform, Plaintiff Fisher Counseling does not get paid for its provision of medical services.

196. Because of Defendants' substandard data security measures, Defendants experienced the Data Breach. Defendants then chose to disconnect the Change Platform from the network.

197. As a result of this disconnection, Plaintiff Fisher Counseling has not received full payment for the medical insurance claims it submitted or has had medical claims outright rejected by insurers. The practice is missing a significant amount in payment without any knowledge about if or when payment will be received.

198. As a result of Defendants' actions, Plaintiff Fisher Counseling and Class members did not receive from Defendants the services that they have paid and/or bargained for, whether directly or indirectly with Defendants. In addition, Plaintiff Fisher Counseling and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and/or have incurred extra costs from switching to another healthcare payment software. Furthermore, Plaintiff Fisher Counseling spent significant time and resources, including, but not limited to, investigating the network outage, physically submitting medical claims, and/or applying for lines of credit as a result of the Change Platform and as a result of its loss/delay of income.

XV. NEW HAMPSHIRE

A. Plaintiff HealthFirst Family Care Center, Inc.

199. Plaintiff HealthFirst is a New Hampshire company with its principal place of business in Franklin, New Hampshire.

200. Plaintiff HealthFirst relies on the Change Platform to provide, among other features, revenue and payment cycle management services.

201. The Change Platform processes most of Plaintiff HealthFirst's medical insurance claims and sends them to insurance companies for evaluation and payment. Once the claims are approved by the insurance company, Plaintiff HealthFirst receives payment.

202. Put simply, without a functioning Change Platform, Plaintiff HealthFirst does not get paid for its provision of medical services.

203. Because of Defendants' substandard data security measures, Defendants experienced the Data Breach. Defendants then chose to disconnect the Change Platform from the network.

204. As a result of this disconnection, Plaintiff HealthFirst has not received full payment for the medical insurance claims it submitted or has had medical claims outright rejected by insurers. The practice is missing a significant amount in payment without any knowledge about if or when payment will be received.

205. As a result of Defendants' actions, Plaintiff HealthFirst and Class members did not receive from Defendants the services that they have paid and/or bargained for, whether directly or indirectly with Defendants. In addition, Plaintiff HealthFirst and Class members have not received payments for their healthcare services or have received late

payments depriving them of the time-value of money and loss of interest and/or have incurred extra costs from switching to another healthcare payment software. Furthermore, Plaintiff HealthFirst spent significant time and resources, including, but not limited to, investigating the network outage, physically submitting medical claims, hiring additional employees, and/or applying for lines of credit as a result of the Change Platform and as a result of its loss/delay of income.

XVI. NEW JERSEY

A. Plaintiff LDK Counseling, LLC

206. Plaintiff LDK Counseling, LLC is a New Jersey limited liability company with its principal place of business in Alpha, New Jersey.

207. Plaintiff LDK relies on the Change Platform to provide, among other features, revenue and payment cycle management services.

208. The Change Platform processes most of Plaintiff LDK's medical insurance claims and sends them to insurance companies for evaluation and payment. Once the claims are approved by the insurance company, Plaintiff LDK receives payment.

209. Put simply, without a functioning Change Platform, Plaintiff LDK does not get paid for its provision of medical services.

210. Because of Defendants' substandard data security measures, Defendants experienced the Data Breach. Defendants then chose to disconnect the Change Platform from the network.

211. As a result of this disconnection, Plaintiff LDK has not received full payment for the medical insurance claims it submitted or has had medical claims outright rejected

by insurers. The practice is missing a significant amount in payment without any knowledge about if or when payment will be received.

212. As a result of Defendants' actions, Plaintiff LDK and Class members did not receive from Defendants the services that they have paid and/or bargained for, whether directly or indirectly with Defendants. In addition, Plaintiff LDK and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and/or have incurred extra costs from switching to another healthcare payment software. Furthermore, Plaintiff LDK spent significant time and resources, including, but not limited to, investigating the network outage, physically submitting medical claims, and/or applying for lines of credit as a result of the Change Platform and as a result of its loss/delay of income.

XVII. NORTH CAROLINA

A. Plaintiff Lisa Ripperton, LCSW, LCAS

213. Plaintiff Lisa Ripperton, LCSW, LCAS is a sole proprietorship with a principal residence in Marion, North Carolina.

214. Plaintiff Ripperton relies on the Change Platform to provide, among other features, revenue and payment cycle management services.

215. The Change Platform processes most of Plaintiff Ripperton's medical insurance claims and sends them to insurance companies for evaluation and payment. Once the claims are approved by the insurance company, Plaintiff Ripperton receives payment.

216. Put simply, without a functioning Change Platform, Plaintiff Ripperton does not get paid for its provision of medical services.

217. Because of Defendants' substandard data security measures, Defendants experienced the Data Breach. Defendants then chose to disconnect the Change Platform from the network.

218. As a result of this disconnection, Plaintiff Ripperton has not received full payment for the medical insurance claims it submitted or has had medical claims outright rejected by insurers. The practice is missing a significant amount in payment without any knowledge about if or when payment will be received.

219. As a result of Defendants' actions, Plaintiff Ripperton and Class members did not receive from Defendants the services that they have paid and/or bargained for, whether directly or indirectly with Defendants. In addition, Plaintiff Ripperton and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and/or have incurred extra costs from switching to another healthcare payment software. Furthermore, Plaintiff Ripperton spent significant time and resources, including but not limited to, investigating the network outage and physically submitting medical claims as a result of the Change Platform and as a result of its loss/delay of income.

XVIII. OREGON

A. Plaintiff Hope and Harmony Counseling, LLC

220. Plaintiff Hope and Harmony Counseling, LLC is an Oregon limited liability company with its principal place of business in Klamath Falls, Oregon, and whose sole member is an Oregon citizen.

221. Plaintiff Hope relies on the Change Platform to provide, among other features, revenue and payment cycle management services.

222. The Change Platform processes most of Plaintiff Hope's medical insurance claims and sends them to insurance companies for evaluation and payment. Once the claims are approved by the insurance company, Plaintiff Hope receives payment.

223. Put simply, without a functioning Change Platform, Plaintiff Hope does not get paid for its provision of medical services.

224. Because of Defendants' substandard data security measures, Defendants experienced the Data Breach. Defendants then chose to disconnect the Change Platform from the network.

225. As a result of this disconnection, Plaintiff Hope has not received full payment for the medical insurance claims it submitted or has had medical claims outright rejected by insurers. The practice is missing a significant amount in payment without any knowledge about if or when payment will be received.

226. As a result of Defendants' actions, Plaintiff Hope and Class members did not receive from Defendants the services that they have paid and/or bargained for, whether directly or indirectly with Defendants. In addition, Plaintiff Hope and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest, and/or have incurred extra costs from switching to another healthcare payment software. Furthermore, Plaintiff Hope spent significant time and resources, including but not limited to, investigating the network

outage and physically submitting medical claims as a result of the Change Platform and as a result of its loss/delay of income.

XIX. PENNSYLVANIA

A. Plaintiff CEPD Psychological Services

227. Plaintiff CEPD Psychological Services is a registered business with its principal place of business in Yardley, Pennsylvania.

228. Plaintiff CEPD relies on the Change Platform to provide, among other features, revenue and payment cycle management services.

229. The Change Platform processes most of Plaintiff CEPD's medical insurance claims and sends them to insurance companies for evaluation and payment. Once the claims are approved by the insurance company, Plaintiff CEPD receives payment.

230. Put simply, without a functioning Change Platform, Plaintiff CEPD does not get paid for its provision of medical services.

231. Because of Defendants' substandard data security measures, Defendants experienced the Data Breach. Defendants then chose to disconnect the Change Platform from the network.

232. As a result of this disconnection, Plaintiff CEPD has not received full payment for the medical insurance claims it submitted or has had medical claims outright rejected by insurers. The practice is missing a significant amount in payment without any knowledge about if or when payment will be received.

233. As a result of Defendants' actions, Plaintiff CEPD and Class members did not receive from Defendants the services that they have paid and/or bargained for, whether

directly or indirectly with Defendants. In addition, Plaintiff CEPD and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and/or have incurred extra costs from switching to another healthcare payment software. Furthermore, Plaintiff CEPD spent significant time and resources, including, but not limited to, investigating the network outage, physically submitting medical claims, and applying for lines of credit as a result of the Change Platform and as a result of its loss/delay of income.

B. Plaintiff East Penn Rheumatology

234. Plaintiff East Penn Rheumatology is a Pennsylvania corporation with its principal place of business in Bethlehem, Pennsylvania.

235. Plaintiff East Penn relies on the Change Platform to provide, among other features, revenue and payment cycle management services.

236. The Change Platform processes most of Plaintiff East Penn's medical insurance claims and sends them to insurance companies for evaluation and payment. Once the claims are approved by the insurance company, Plaintiff East Penn receives payment.

237. Put simply, without a functioning Change Platform, Plaintiff East Penn does not get paid for its provision of medical services.

238. Because of Defendants' substandard data security measures, Defendants experienced the Data Breach. Defendants then chose to disconnect the Change Platform from the network.

239. As a result of this disconnection, Plaintiff East Penn has not received full payment for the medical insurance claims it submitted or has had medical claims outright

rejected by insurers. The practice is missing a significant amount in payment without any knowledge about if or when payment will be received.

240. As a result of Defendants' actions, Plaintiff East Penn and Class members did not receive from Defendants the services that they have paid and/or bargained for, whether directly or indirectly with Defendants. In addition, Plaintiff East Penn and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and/or have incurred extra costs from switching to another healthcare payment software. Furthermore, Plaintiff East Penn spent significant time and resources, including, but not limited to, investigating the network outage, physically submitting medical claims, and/or applying for lines of credit as a result of the Change Platform and as a result of its loss/delay of income.

C. Plaintiff Koka Cardiology

241. Plaintiff Koka Cardiology is a Pennsylvania corporation with its principal place of business in Philadelphia, Pennsylvania.

242. Plaintiff Koka relies on the Change Platform to provide, among other features, revenue and payment cycle management services.

243. The Change Platform processes most of Plaintiff Koka's medical insurance claims and sends them to insurance companies for evaluation and payment. Once the claims are approved by the insurance company, Plaintiff Koka receives payment.

244. Put simply, without a functioning Change Platform, Plaintiff Koka does not get paid for its provision of medical services.

245. Because of Defendants' substandard data security measures, Defendants experienced the Data Breach. Defendants then chose to disconnect the Change Platform from the network.

246. As a result of this disconnection, Plaintiff Koka has not received full payment for the medical insurance claims it submitted or has had medical claims outright rejected by insurers. The practice is missing a significant amount in payment without any knowledge about if or when payment will be received.

247. As a result of Defendants' actions, Plaintiff Koka and Class members did not receive from Defendants the services that they have paid and/or bargained for, whether directly or indirectly with Defendants. In addition, Plaintiff Koka and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and/or have incurred extra costs from switching to another healthcare payment software. Furthermore, Plaintiff Koka spent significant time and resources, including but not limited to, investigating the network outage and physically submitting medical claims as a result of the Change Platform and as a result of its loss/delay of income.

D. Plaintiff Summit Psychiatric Services, LLC

248. Plaintiff Summit Psychiatric Services, LLC is a Pennsylvania limited liability company with its principal place of business in Clarks Summit, Pennsylvania whose sole member is a Pennsylvania citizen.

249. Plaintiff Summit Psychiatric relies on the Change Platform to provide, among other features, revenue and payment cycle management services.

250. The Change Platform processes most of Plaintiff Summit Psychiatric's medical insurance claims and sends them to insurance companies for evaluation and payment. Once the claims are approved by the insurance company, Plaintiff Summit Psychiatric receives payment.

251. Put simply, without a functioning Change Platform, Plaintiff Summit Psychiatric does not get paid for its provision of medical services.

252. Because of Defendants' substandard data security measures, Defendants experienced the Data Breach. Defendants then chose to disconnect the Change Platform from the network.

253. As a result of this disconnection, Plaintiff Summit Psychiatric has not received full payment for the medical insurance claims it submitted or has had medical claims outright rejected by insurers. The practice is missing a significant amount in payment without any knowledge about if or when payment will be received.

254. As a result of Defendants' actions, Plaintiff Summit Psychiatric and Class members did not receive from Defendants the services that they have paid and/or bargained for, whether directly or indirectly with Defendants. In addition, Plaintiff Summit Psychiatric and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and/or have incurred extra costs from switching to another healthcare payment software. Furthermore, Plaintiff Summit Psychiatric spent significant time and resources, including but not limited to, investigating the network outage, physically submitting medical claims,

and/or applying for lines of credit as a result of the Change Platform and as a result of its loss/delay of income.

E. Plaintiff Wiemer Family Podiatry, LLC

255. Plaintiff Wiemer Family Podiatry, LLC is a Pennsylvania limited liability company with its principal place of business in Havertown, Pennsylvania whose sole member is a Pennsylvania citizen.

256. Plaintiff Wiemer relies on the Change Platform to provide, among other features, revenue and payment cycle management services.

257. The Change Platform processes most of Plaintiff Wiemer's medical insurance claims and sends them to insurance companies for evaluation and payment. Once the claims are approved by the insurance company, Plaintiff Wiemer receives payment.

258. Put simply, without a functioning Change Platform, Plaintiff Wiemer does not get paid for its provision of medical services.

259. Because of Defendants' substandard data security measures, Defendants experienced the Data Breach. Defendants then chose to disconnect the Change Platform from the network.

260. As a result of this disconnection, Plaintiff Wiemer has not received full payment for the medical insurance claims it submitted or has had medical claims outright rejected by insurers. The practice is missing a significant amount in payment without any knowledge about if or when payment will be received.

261. As a result of Defendants' actions, Plaintiff Wiemer and Class members did not receive from Defendants the services that they have paid and/or bargained for, whether

directly or indirectly with Defendants. In addition, Plaintiff Wiemer and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and/or have incurred extra costs from switching to another healthcare payment software. Furthermore, Plaintiff Wiemer spent significant time and resources, including but not limited to, investigating the network outage, physically submitting medical claims, and/or applying for lines of credit as a result of the Change Platform and as a result of its loss/delay of income.

XX. RHODE ISLAND

A. Plaintiff Frank P. Maggiacomo, D.O., Inc./MOC

262. Plaintiff Frank P. Maggiacomo, D.O., Inc./MOV is a Rhode Island corporation with its principal place of business in Cranston, Rhode Island.

263. Plaintiff Maggiacomo relies on the Change Platform to provide, among other features, revenue and payment cycle management services.

264. The Change Platform processes most of Plaintiff Maggiacomo's medical insurance claims and sends them to insurance companies for evaluation and payment. Once the claims are approved by the insurance company, Plaintiff Maggiacomo receives payment.

265. Put simply, without a functioning Change Platform, Plaintiff Maggiacomo does not get paid for its provision of medical services.

266. Because of Defendants' substandard data security measures, Defendants experienced the Data Breach. Defendants then chose to disconnect the Change Platform from the network.

267. As a result of this disconnection, Plaintiff Maggiacomo has not received full payment for the medical insurance claims it submitted or has had medical claims outright rejected by insurers. The practice is missing a significant amount in payment without any knowledge about if or when payment will be received.

268. As a result of Defendants' actions, Plaintiff Maggiacomo and Class members did not receive from Defendants the services that they have paid and/or bargained for, whether directly or indirectly with Defendants. In addition, Plaintiff Maggiacomo and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and/or have incurred extra costs from switching to another healthcare payment software. Furthermore, Plaintiff Maggiacomo spent significant time and resources, including but not limited to, investigating the network outage, physically submitting medical claims, and/or applying for lines of credit as a result of the Change Platform and as a result of its loss/delay of income.

XXI. TEXAS

A. Plaintiff Crom Rehabilitation LLC d/b/a Elation Physical Therapy

269. Plaintiff Crom Rehabilitation LLC d/b/a Elation Physical Therapy is a Texas professional limited liability company with its principal place of business in Houston, Texas and whose sole member is a Texas citizen.

270. Plaintiff Elation PT relies on the Change Platform to provide, among other features, revenue and payment cycle management services.

271. The Change Platform processes most of Plaintiff Elation PT's medical insurance claims and sends them to insurance companies for evaluation and payment. Once the claims are approved by the insurance company, Plaintiff Elation PT receives payment.

272. Put simply, without a functioning Change Platform, Plaintiff Elation PT does not get paid for its provision of medical services.

273. Because of Defendants' substandard data security measures, Defendants experienced the Data Breach. Defendants then chose to disconnect the Change Platform from the network.

274. As a result of this disconnection, Plaintiff Elation PT has not received full payment for the medical insurance claims it submitted or has had medical claims outright rejected by insurers. The practice is missing a significant amount in payment without any knowledge about if or when payment will be received.

275. As a result of Defendants' actions, Plaintiff Elation PT and Class members did not receive from Defendants the services that they have paid and/or bargained for, whether directly or indirectly with Defendants. In addition, Plaintiff Elation PT and Class members have not received payments for their healthcare services or have received late payments, depriving them of the time-value of money and loss of interest and/or have incurred extra costs from switching to another healthcare payment software. Furthermore, Plaintiff Elation PT spent significant time and resources, including but not limited to, investigating the network outage and physically submitting medical claims as a result of the Change Platform and its loss/delay of income.

B. Plaintiff M.P. Counseling Services, PLLC

276. Plaintiff M.P. Counseling Services is a Texas professional limited liability company with its principal place of business in Longview, Texas, and whose sole member is a Texas citizen.

277. Plaintiff M.P. Counseling relies on the Change Platform to provide, among other features, revenue and payment cycle management services.

278. The Change Platform processes most of Plaintiff M.P. Counseling's medical insurance claims and sends them to insurance companies for evaluation and payment. Once the claims are approved by the insurance company, Plaintiff M.P. Counseling receives payment.

279. Put simply, without a functioning Change Platform, Plaintiff M.P. Counseling does not get paid for its provision of medical services.

280. Because of Defendants' substandard data security measures, Defendants experienced the Data Breach. Defendants then chose to disconnect the Change Platform from the network.

281. As a result of this disconnection, Plaintiff M.P. Counseling has not received full payment for the medical insurance claims it submitted or has had medical claims outright rejected by insurers. The practice is missing a significant amount in payment without any knowledge about if or when payment will be received.

282. As a result of Defendants' actions, Plaintiff M.P. Counseling and Class members did not receive from Defendants the services that they have paid and/or bargained for, whether directly or indirectly with Defendants. In addition, Plaintiff M.P. Counseling

and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and/or have incurred extra costs from switching to another healthcare payment software. Furthermore, Plaintiff M.P. Counseling spent significant time and resources, including but not limited to, investigating the network outage and physically submitting medical claims as a result of the Change Platform and its loss/delay of income.

XXII. VERMONT

A. Plaintiff Northern Vermont Dermatology, PLC

283. Plaintiff Northern Vermont Dermatology, PLC is a Vermont professional limited liability company with its principal place of business in Saint Albans, Vermont whose sole member is a Vermont citizen.

284. Plaintiff NVD relies on the Change Platform to provide, among other features, revenue and payment cycle management services.

285. The Change Platform processes most of Plaintiff NVD's medical insurance claims and sends them to insurance companies for evaluation and payment. Once the claims are approved by the insurance company, Plaintiff NVD receives payment.

286. Put simply, without a functioning Change Platform, Plaintiff NVD does not get paid for its provision of medical services.

287. Because of Defendants' substandard data security measures, Defendants experienced the Data Breach. Defendants then chose to disconnect the Change Platform from the network.

288. As a result of this disconnection, Plaintiff NVD has not received full payment for the medical insurance claims it submitted or has had medical claims outright rejected by insurers. The practice is missing a significant amount in payment without any knowledge about if or when payment will be received.

289. As a result of Defendants' actions, Plaintiff NVD and Class members did not receive from Defendants the services that they have paid and/or bargained for, whether directly or indirectly with Defendants. In addition, Plaintiff NVD and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and/or have incurred extra costs from switching to another healthcare payment software. Furthermore, Plaintiff NVD spent significant time and resources, including but not limited to, investigating the network outage, physically submitting medical claims, and/or applying for lines of credit as a result of the loss/delay of income.

XXIII. WASHINGTON

A. Plaintiff Dov Wills, PLLC

290. Plaintiff Dov Wills, PLLC is a Washington sole proprietorship with a residence in Lynwood, Washington.

291. Plaintiff Wills relies on the Change Platform to provide, among other features, revenue and payment cycle management services.

292. The Change Platform processes Plaintiff Wills's medical insurance claims and sends them to insurance companies for evaluation and payment. Once the claims are approved by the insurance company, Plaintiff Wills receives payment.

293. Put simply, without a functioning Change Platform, Plaintiff Wills does not get paid for its provision of medical services.

294. Because of Defendants' substandard data security measures, Defendants experienced the Data Breach. Defendants then chose to disconnect the Change Platform from the network.

295. As a result of this disconnection, Plaintiffs Wills received delayed payments for the medical insurance claims it submitted or has had medical claims outright rejected by insurers.

296. As a result of Defendants' actions, Plaintiff Wills and Class members did not receive from Defendants the services that they have paid and/or bargained for, whether directly or indirectly with Defendants. In addition, Plaintiff Wills and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and/or have incurred extra costs from switching to another healthcare payment software. Furthermore, Plaintiff Wills spent significant time and resources, including, but not limited to, investigating the network outage, physically completing and submitting medical claims, and/or applying for lines of credit as a result of the Change Platform and as a result of its loss/delay of income.

DEFENDANTS

297. Defendant Change Healthcare Inc. is a publicly traded company incorporated in Delaware with its principal place of business in Nashville, Tennessee. It became a subsidiary of UnitedHealth Group Incorporated in 2022 and is operated by Optum, Inc., another UHG subsidiary.

298. Defendant Optum, Inc. maintains its principal place of business in Eden Prairie, Minnesota and is incorporated in Delaware.

299. Defendant UnitedHealth Group Incorporated is a Delaware corporation with its principal place of business in Minnetonka, Minnesota. UHG exercises control over the management of the Change cybersecurity systems as evidenced by, inter alia, UHG's response to the Data Breach as alleged herein.

FACTUAL ALLEGATIONS

300. As referenced above, UHG is a healthcare conglomerate consisting of UnitedHealthcare, along with three Optum divisions: Optum Health, OptumInsight, and Optum Rx.[14]

301. Optum Health offers direct care services through local medical groups and ambulatory care systems, providing primary, specialty, urgent, and surgical care to nearly 103 million consumers. Optum Health serves a diverse clientele, including employers, health systems, government agencies, and health plans.[15]

302. OptumInsight offers a range of solutions including data, analytics, research, consulting, technology, and managed services to hospitals, physicians, health plans, governments, and life sciences companies. This division assists customers in lowering

[14] *See* Abelson & Creswell, *supra* note 1.
[15] *Optum: Technology and data-enabled care delivery*, UNITEDHEALTH GROUP, https://www.unitedhealthgroup.com/people-and-businesses/businesses/optum.html (last visited July 16, 2024).

administrative expenses, complying with regulations, enhancing clinical performance, and reimagining operational processes.[16]

303. Optum Rx provides a comprehensive range of pharmacy services aimed at making medications more accessible and enhancing consumer experiences. Annually, it services over 1.5 billion adjusted retail, mail, and specialty drug prescriptions. Optum Rx solutions are grounded in evidence-based clinical guidelines. As part of its regular operations, Optum Rx collects and retains payment and health information from both patients and benefit sponsors.[17]

304. Defendant Change Healthcare operates as a health technology company offering pharmacies and healthcare providers in the United States electronic tools for processing claims and managing essential payment and revenue procedures.

305. Change Healthcare is among the largest prescription medication processors in the United States, managing billing for over 67,000 pharmacies nationwide and facilitating 15 billion healthcare transactions annually.[18]

306. As referenced above, in October 2022, UHG finalized its acquisition of Change Healthcare, aiming to integrate it with OptumInsight.[19]

---

[16] *Id.*
[17] *Id.*
[18] Zack Whittaker, *UnitedHealth confirms ransomware gang behind Change Healthcare hack amid ongoing pharmacy outages*, TECHCRUNCH (Feb. 29, 2024, 9:15 AM), https://techcrunch.com/2024/02/29/unitedhealth-change-healthcare-ransomware-alphv-blackcat-pharmacy-outages/.
[19] James Farrell, *Change Healthcare Blames 'Blackcat' Group for Cyber Attack That Disrupted Pharmacies and Health Systems*, FORBES (Feb. 29, 2024, 1:18 PM), https://www.forbes.com/sites/jamesfarrell/2024/02/29/change-healthcare-blames-

307. Accordingly, the President of UHG and CEO of Optum said that the combination of Change's and Optum's services "will help streamline and inform the vital clinical, administrative and payment processes on which health care providers and payers depend to serve patients."[20]

308. Therefore, as part of their routine operations, Optum and Change (and, in turn, their parent company, UHG) receive and/or retain patients' payment and health insurance details, along with their sensitive health information.

309. As referenced in UHG's most recent annual report submitted to the SEC, UHG "acquired all of the outstanding common shares of Change Healthcare." Consequently, Change Healthcare, just like Optum, is now wholly owned by UHG and operates under the umbrella of UHG's corporate structure.

310. As such, UnitedHealth Group Incorporated is accountable for supervising the cybersecurity practices and protocols of all UHG companies within its corporate framework.

Change's Role in the Healthcare Industry.

311. Change Healthcare is a healthcare technology company that provides data-driven and analytics-driven solutions for clinical, financial, administrative, and patient

blackcat-group-for-cyber-attack-that-disrupted-pharmacies-and-health-systems/?sh=589769fc1c4d.

[20] *OptumInsight and Change Healthcare Combine to Advance a More Modern, Information and Technology-Enabled Health Care Platform*, UNITEDHEALTH GROUP (Jan. 6, 2021), https://www.unitedhealthgroup.com/newsroom/2021/2021-01-06-optuminsight-and-change-healthcare-combine.html (last visited July 16, 2024).

management to healthcare providers.[21] It holds itself out as providing "data and analytics, plus patient engagement and collaboration tools" to "providers and payers [to] optimize workflows, access the right information at the right time, and support the safest and most clinically appropriate care."[22] Change is one of the largest processors of prescription medications in the United States and handles billing for more than 67,000 pharmacies across the country.[23] And it is also the nation's largest clearinghouse for insurance claims and payments – connecting more than 800,000 providers and 2,100 payers.[24] In total, Change handles 15 billion healthcare transactions annually or about one-in-three U.S. patient records.[25]

312. Change is the backbone of the patient billing life cycle. When a patient visits a physician for a medical consultation, the physician documents the visit and submits charges on a medical claim by applying appropriate codes that align with that visit.[26] After

---

[21] *OptumInsight and Change Healthcare Combine to Advance a More Modern, Information and Technology-Enabled Health Care Platform*, OPTUM (Jan. 6, 2021), https://www.optum.com/en/about-us/news/page.hub.optuminsight-change-healthcare-combine.html.

[22] *The Change Healthcare Platform*, CHANGE HEALTHCARE, https://www.changehealthcare.com/platform (last visited July 16, 2024).

[23] Zack Whittaker, *UnitedHealth confirms ransomware gang behind Change Healthcare hack amid ongoing pharmacy outages*, TECHCRUNCH (Feb. 29, 2024, 9:15 AM) https://techcrunch.com/2024/02/29/unitedhealth-change-healthcare-ransomware-alphv-blackcat-pharmacy-outages/.

[24] *Claiming and Remittance*, CHANGE HEALTHCARE, https://www.changehealthcare.com/medical-network/claiming-remittance (last visited July 16, 2024).

[25] *How to Deliver High-Performance Healthcare Marketing*, CHANGE HEALTHCARE, https://www.changehealthcare.com/insights/deliver-high-performance-healthcare-marketing (last visited July 16, 2024).

[26] Health Subcommittee Hearing: "Examining Health Sector Cybersecurity in the Wake

the billing team reviews for errors, the claim is sent to Change (i.e., clearinghouse) for additional accuracy checks and processing.[27] Change then transfers the medical claim to the insurer or payer who has 45 days to process the claim for payment or deny it.[28] If approved, the payer sends payment to the practice and an ERA, which outlines the claim, the allowable amounts paid, or denials, that the practice uses to reconcile the patient's account balance.[29] For example, if a practice bills $300 for a medical consultation and the insurance allowable amount is $150, then the insurance company will pay $150 and the practice will either seek the remaining $150 from the patient or write it off.[30]

313. As a result of the scope of Change's network and its specialized position within the billing life cycle, when Defendants disconnected the Change Platform following the Data Breach, "it affected all practices' ability to send claims early in the life cycle and forced physicians to hold claims in the billing bucket until alternative clearinghouse connections were established."[31]

314. Change's role in the healthcare industry was reinforced in 2022 after it was purchased by UHG—the largest health insurance provider in the United States—and merged with Optum. In 2022, despite opposition from the Department of Justice and other

---

of the Change Healthcare Attack: Hearing Before the Subcomm. on Energy and Commerce (Apr. 16, 2024) (Statement of Adam Bruggeman, MD), available at: Adam_Bruggeman_Witness_Testimony_04_16_2024_7c546a4de0.pdf (d1dth6e84htgma.cloudfront.net).

[27] *Id.* at 2.

[28] *Id.*

[29] *Id.*

[30] *Id.*

[31] *Id.*

organizations like the American Hospital Association, a federal judge greenlighted UHG's $13 billion transaction of Change to merge with Optum.[32] Opponents of the blockbuster transaction took issue with, among other things, that patients' healthcare data would be consolidated under one roof and shared between the largest health insurer, largest claims processing company, and the third largest pharmacy benefits manager in America.[33]

Defendants' Privacy Practices

315. In the regular course of business, Change—and through their related corporate ownership, Defendants—store patients' highly sensitive health information collected from a substantial number of clients like Medicare, pharmacies, healthcare providers, and so on. This includes patients' full names, phone numbers, addresses, Social Security numbers, emails, medical records, dental records, payment information, claims information, insurance records, and much more.

316. Given the amount and sensitive nature of the data it stores, Change assures providers that it has various processes and policies in place to protect their clients'/patients' sensitive information: "Keeping our customers' information secure is a top priority for Change Healthcare. We dedicate extensive resources to make sure personal medical and

[32] Susan Morse, *DOJ, States Drop Appeal of Optum and Change Merger*, HEALTHCARE FINANCE (Mar. 22, 2023), https://www.healthcarefinancenews.com/news/doj-states-drop-appeal-optum-and-change-merger.

[33] Melinda Hatton, *AHA Statement on Department of Justice Decision on Proposed Unitedhealth Group Acquisition of Change Healthcare*, AMERICAN HOSPITAL ASSOCIATION (Feb. 24, 2022), https://www.aha.org/press-releases/2022-02-24-aha-statement-department-justice-decision-proposed-unitedhealth-group.

financial information is secure and we strive to build a company culture that reinforces trust at every opportunity."[34]

317. Given its representations and experience handling highly sensitive PII and PHI, Change understood the need to protect patients' PII and PHI and prioritize data security.

318. As part of its routine operations, UHG retains highly sensitive health information from various sources such as Medicare, pharmacies, healthcare providers, and others. This information comprises patients' complete identities, contact details, Social Security numbers, medical and dental records, payment and claims data, insurance records, and more.

319. Given the extensive amount and sensitive nature of the data they handle, Defendants maintain privacy policies outlining the usage and disclosure of confidential and personal information. UHG and Optum adhere to the same "Privacy Policy," which assures the public—such as Provider Plaintiffs and NCPA Members—that Defendants have implemented "administrative, technical, and physical safeguards" to safeguard patients' information. Their "Social Security Number Protection Policy" explicitly states their commitment to preserving the confidentiality of Social Security numbers received or collected during business operations. Defendants also pledge to limit access to Social Security numbers to lawful purposes and to prohibit unlawful disclosure. Change similarly

[34] *Accreditations & Certifications*, CHANGE HEALTHCARE, https://www.changehealthcare.com/accreditations-certifications(last visited July 16, 2024).

assures that it implements and maintains security measures—organizational, technical, and administrative—to protect processed data from unauthorized access, destruction, loss, alteration, or misuse. These measures aim to uphold the integrity and confidentiality of data, including personal information.[35]

320. Accordingly, as stated on its website, Change assures the following:

> 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. We evaluate and update these measures on an ongoing basis. Your Personal Information is only accessible to personnel who need to access it to perform their duties.[36]

The patients of Provider Plaintiffs, NCPA Members, and Class members provided Defendants with their PII and PHI, on which Defendants rely to conduct their routine business operations.

The Data Breach

321. On February 21, 2024, in a SEC filing, Defendants announced that "a suspected nation-state associated cyber security threat actor had gained access to some of the Change Healthcare information technology systems."[37] After detecting the breach, Defendants claimed to have "proactively isolated the impacted systems from other

[35] *Privacy Notice*, CHANGE HEALTHCARE, https://www.changehealthcare.com/privacy-notice (last visited July 16, 2024).
[36] https://www.changehealthcare.com/privacy-notice (last visited Mar. 11, 2024).
[37] *UnitedHealth Group Incorporation Form 8-K*, SEC (Feb. 21, 2024), https://www.sec.gov/Archives/edgar/data/731766/000073176624000045/unh-20240221.htm.

connecting systems . . . ."[38] Defendants also said they were "working with law enforcement" and allegedly "notified customers, clients and certain government agencies" of the Breach.[39] UHG disclosed that the "network interruption [was] specific to Change Healthcare . . . ."[40]

322. Blackcat has disclosed that the data exfiltrated in the Data Breach includes millions of: "active US military/navy personnel PII," "medical records," "dental records," "payments information," "Claims information," "Patients PII including Phone numbers/addresses/SSN/emails/etc…," "3000+ source code files for Change Health solutions…," "Insurance records," and "many many more." Blackcat warned Defendants that they were "walking on a very thin line be careful you just might fall over."

323. At the May 1, 2024 Subcommittee on Oversight and Investigation Hearing, UHG CEO Andrew Witty estimated that one-third of Americans were impacted by the Data Breach.[41] He also revealed that Blackcat gained access to Defendants' network because of a lack of multi-factor authentication ("MFA") on a Change server. More specifically, Blackcat used compromised credentials to infiltrate Defendants' network through the externally facing Change server.[42]

---

[38] *Id.*
[39] *Id.*
[40] *Id.*
[41] Ashley Capoot, *UnitedHealth CEO estimates one-third of Americans could be impacted by Change Healthcare cyberattack*, CNBC (May 20, 2024), https://www.cnbc.com/2024/05/01/unitedhealth-ceo-one-third-of-americans-could-be-impacted-by-change-healthcare-cyberattack.html.
[42] *Id.*

324. Defendants intentionally disconnected the Change Platform following the Data Breach. Through the Change Platform, healthcare providers—who have paid for Defendants' Change Platform—submit insurance claims. These claims are sent to health insurance companies to evaluate and process. Providers then receive reimbursement payments and ERAs from the insurance company.

325. Defendants intentionally made the Change Platform inoperable from the time of the Data Breach through at least mid-March. While certain systems have been brought back online, as of the filing of this Complaint, the Change Platform is still not operating at pre-incident levels.[43]

326. The Change Platform handles 15 billion healthcare transactions (or about one-in-three U.S. patient records). That means that the normal method of transmitting claims for payment was disrupted for a huge swath of providers' claims. Moreover, many providers only used Change for claims submission, meaning that for those providers, the impact was to completely stop the flow of payments.

327. The impact of the Data Breach is enormous and not yet fully known, and its effects are currently being felt by healthcare providers nationwide.

The Aftermath of the Data Breach

328. As a result of the Data Breach, Defendants disconnected certain systems, including the Change Platform used by healthcare providers nationwide in connection with

[43] *Information on the Change Healthcare Cyber Response*, UNITEDHEALTH GROUP, https://www.unitedhealthgroup.com/changehealthcarecyberresponse (last visited July 16, 2024) (listing the updated ERA Payer List for Change Healthcare customers).

claims processing, payment, and treatment. Defendants did this without an adequate substitute. This decision is decimating healthcare practices nationwide. Indeed, UHG CEO Witty acknowledged that "shutting down many Change environments was extremely disruptive[.]"[44]

329. Because Defendants disconnected the Change Platform, many healthcare providers lost their primary (and in some cases their only) source of processing payments for their services through patients' healthcare plans and thus did not receive payment. Healthcare providers had to absorb these upfront costs.

330. A dwindling account balance coupled with outstanding reimbursement put many healthcare providers in a precarious position. For instance, Arlington Urgent Care, a chain of five urgent care centers around Columbus, Ohio, had about $650,000 in unpaid insurance reimbursements. The owners took lines of credit from banks and used their personal savings to afford employee payroll, rent, and other expenses.[45] Other healthcare providers racked up duplicated payment software charges. Florida Cancer Specialists and Research Institute in Gainesville switched to two other healthcare software platforms because "it spends $300 million a month on chemotherapy and other drugs for patients whose treatments cannot be delayed."[46] And some healthcare providers cut resources for

[44] Finance Committee Hearing: "Hacking America's Health Care: Assessing the Change Healthcare Cyber Attack and What's Next" (May 1, 2024) (Statement of Andrew Witty), available at: https://www.finance.senate.gov/imo/media/doc/0501_witty_testimony.pdf.
[45] Reed Abelson & Julie Creswell, *Cyberattack Paralyzes the Largest U.S. Healthcare Payment System*, NYTIMES (Mar. 7, 2024), https://www.nytimes.com/2024/03/05/health/cyberattack-healthcare-cash.html.
[46] *Id.*

patients to persevere through the shutdown. A Philadelphia-based primary care practice with 20 clinicians mailed off "hundreds and hundreds" of pages Medicare claims and was contemplating cutting expenses by "reducing the supply of vaccines the clinic has on hand."[47]

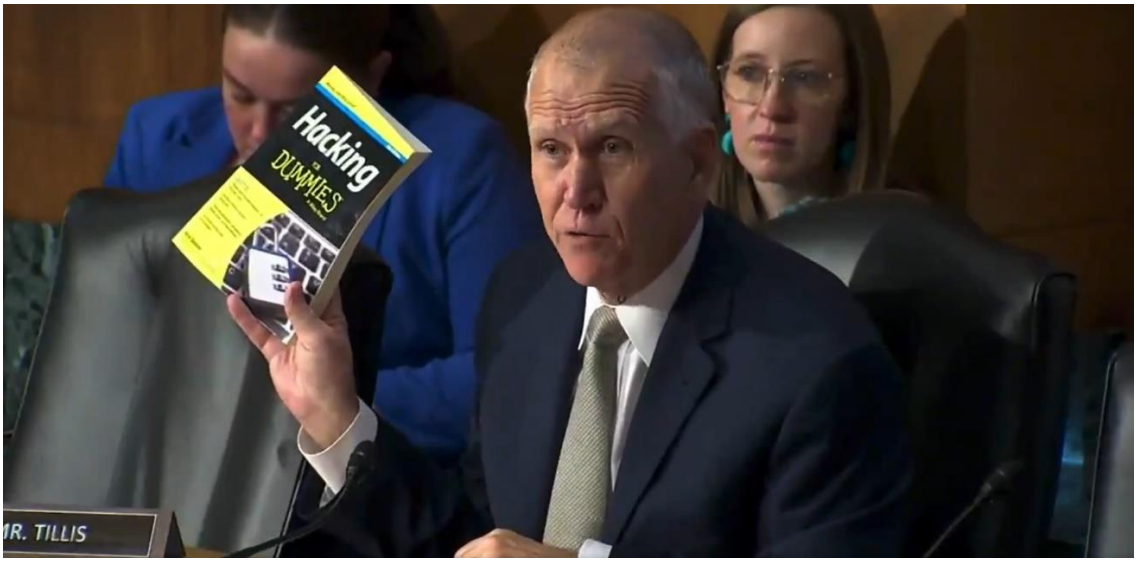
331. Healthcare providers did not receive Defendants' services that they paid for and/or bargained for, whether indirectly or directly, and without these services, these providers and practices are struggling to care for patients and are losing money.

The Data Breach Was Preventable

332. As Senator Wyden exclaimed during the Senate hearing, "this hack could have been stopped with cybersecurity 101."[48] Indeed, as CEO Witty sheepishly revealed, Change lacked necessary MFA on the server that was breached.[49]

333. Senator Thom Tillis further confirmed the preventability of this Data Breach. Waiving a copy of "Hacking for Dummies," Sen. Tillis emphasized that "[t]his is some basic stuff that was missed, so shame on internal audit, external audit and your systems folks tasked with redundancy, they're not doing their job."

[47] *Id.*
[48] Pietje Kobus, *UnitedHealth CEO Testifies on Cyberattack Before Senate*, HEALTHCARE INNOVATION (May 2, 2024), https://www.hcinnovationgroup.com/cybersecurity/news/55036427/unitedhealth-ceo-testifies-on-cyberattack-before-senate.
[49] *Id.*



1. Sen. Tillis holding a copy of "Hacking for Dummies" at the May 1, 2024, committee hearing regarding the Change Data Breach.

334. Despite the foreseeability of the Data Breach, this cyber disaster occurred in part because, as CEO Witty highlighted, Change is a 40-year-old company with outdated and differing generations of technology.

335. As a 40-year-old company with 40-year-old technology, Change's cybersecurity practices and policies were inadequate and fell short of the industry-standard measures that should have been implemented long before the Data Breach occurred. This is especially true given that the healthcare industry is frequently one of the most targeted sectors for cyberattacks. Attacks using stolen credentials have increased precipitously over the last several years.

336. Healthcare providers and their affiliates like Defendants are prime targets because of the information they collect and store, including financial information of patients, login credentials, insurance information, medical records and diagnoses, and

personal information of employees and patients—all extremely valuable on underground markets.

337. This was known and obvious to Defendants as they observed frequent public announcements of data breaches affecting healthcare providers and knew that information of the type they collect, maintain, and store is highly coveted and a frequent target of hackers.

338. UHG acknowledged this in its Form 10-K SEC filing:

> If we or third parties we rely on sustain cyber-attacks or other privacy or data security incidents resulting in disruption to our operations or the disclosure of protected personal information or proprietary or confidential information, we could suffer a loss of revenue and increased costs, negative operational affects, exposure to significant liability, reputational harm and other serious negative consequences.
>
> We routinely process, store and transmit large amounts of data in our operations, including protected personal information subject to privacy, security or data breach notification laws, as well as proprietary or confidential information relating to our business or third parties. . . . We are regularly the target of attempted cyber-attacks and other security threats and have previously been, and may in the future be, subject to compromises of the information technology systems we use, information we hold, or information held on our behalf by third parties. While we have programs in place to detect, contain and respond to data security incidents and provide employee awareness training regarding phishing, malware and other cyber threats to protect against cyber risks and security incidents, we expect that we will continue to experience these incidents, some of which may negatively affect our business.[50]

[50] *UnitedHealth Group Form 10-K*, SEC (Feb. 28, 2024), https://www.sec.gov/ix?doc=/Archives/edgar/data/0000731766/000073176624000081/unh-20231231.htm.

339. It is well known that use of stolen credentials has long been the most popular and effective method of gaining authorized access to a company's internal networks and that companies should activate defenses to prevent such attacks.

340. According to the Federal Bureau of Investigation (FBI), phishing schemes designed to induce individuals to reveal personal information, such as network passwords, were the most common type of cybercrime in 2020, with such incidents nearly doubling in frequency between 2019 and 2020.[51] According to Verizon's 2021 Data Breach Investigations Report, 43% of breaches stemmed from phishing and/or pretexting schemes.[52]

341. The risk is so prevalent for healthcare providers that on October 28, 2020, the FBI and two federal agencies issued a "Joint Cybersecurity Advisory" warning that they have "credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers."[53] The Cybersecurity and Infrastructure Security Agency (CISA), the Department of Health and Human Services (HHS), and the FBI issued

[51] *2020 Internet Crime Report*, FBI, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (last visited July 16, 2024).
[52] *2021 DBIR Master's Guide*, VERIZON, https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/ (subscription required) (last visited July 16, 2024).
[53] *Ransomware Activity Targeting the Healthcare and Public Health Sector*, JOINT CYBERSECURITY ADVISORY, https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf (last visited July 16, 2024).

the advisory to warn healthcare providers to take "timely and reasonable precautions to protect their networks from these threats."[54]

342. There are two primary ways to mitigate the risk of stolen credentials: user education and technical security barriers. User education is the process of making employees or other users of a network aware of common disclosure schemes and implementing company-wide policies requiring the request or transfer of sensitive personal or financial information only through secure sources to known recipients. For example, a common phishing e-mail is an "urgent" request from a company "executive" requesting confidential information in an accelerated timeframe. The request may come from an e-mail address that appears official but contains only one different number or letter. Other phishing methods include baiting a user to click a malicious link that redirects them to a nefarious website or to download an attachment containing malware.

343. User education provides the easiest method to assist in properly identifying fraudulent "spoofing" e-mails and prevent unauthorized access of sensitive internal information. According to September 2020 guidance from CISA, organizations housing sensitive data should "[i]mplement a cybersecurity user awareness and training program that includes guidance on how to identify and report suspicious activity" and conduct "organization-wide phishing tests to gauge user awareness and reinforce the importance of identifying potentially malicious emails."[55]

---

[54] *Id.*

[55] *Ransonware Guide September 2020,* CISA, available at: https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf.

344. Through technical security barriers, companies can also greatly reduce the flow of fraudulent e-mails by installing software that scans all incoming messages for harmful attachments or malicious content and implementing certain security measures governing e-mail transmissions, including Sender Policy Framework (SPF) (e-mail authentication method used to prevent spammers from sending messages on behalf of a company's domain), DomainKeys Identified Mail (DKIM) (e-mail authentication method used to ensure messages are not altered in transit between the sending and recipient servers), and Domain-based Message Authentication, Reporting and Conformance (DMARC), which "builds on the widely deployed [SPF] and [DKIM] protocols, adding a reporting function that allows senders and receivers to improve and monitor protection of the domain from fraudulent email."[56]

345. Companies can also take steps to ensure that user passwords are not recycled across platforms, so that a breach, for example, of a user's Netflix password would not yield a password that could also be used to access that user's work account at Change.

346. Additionally, because the goal of these schemes is to gain an employee's login credentials to access a company's network, there are industry-standard measures that companies can implement to greatly reduce unauthorized access, even if an individual's login credentials are disclosed. For example, MFA is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login. This could include entering a code from the user's smartphone,

[56] *Id.*

answering a security question, or providing a biometric indicator such as a fingerprint or facial recognition—in addition to entering a username and password. Thus, even if hackers obtain an employee's username and password, access to the company's system is thwarted because they do not have access to the additional authentication methods.

347. In addition to mitigating the risk of stolen credentials, the CISA guidance encourages organizations to prevent unauthorized access by:

(a) Conducting regular vulnerability scanning to identify and address vulnerabilities, particularly on internet-facing devices;

(b) Regularly patching and updating software to latest available versions, prioritizing timely patching of internet-facing servers and software processing internet data;

(c) Ensuring devices are properly configured and that security features are enabled;

(d) Employing best practices for use of Remote Desktop Protocol (RDP) as threat actors often gain initial access to a network through exposed and poorly secured remote services; and

(e) Disabling operating system network file sharing protocol known as Server Message Block (SMB), which is used by threat actors to travel through a network to spread malware or access sensitive data.[57]

[57] *Id.* at 4.

348. The CISA guidance further recommends use of a centrally managed antivirus software utilizing automatic updates that will protect all devices connected to a network (as opposed to requiring separate software on each individual device), as well as implementing a real-time intrusion detection system that will detect potentially malicious network activity that occurs prior to ransomware deployment.[58] Likewise, the principle of least privilege (POLP) to all systems should be applied to all systems so that users only have the access they need to perform their jobs.[59]

349. Not only should Defendants have had measures in place to prevent compromise in the first place, Defendants should have also properly siloed their systems so that a bad actor would be unable to escalate privileges and move laterally through Defendants' systems. A data silo can occur when an organization manages data separately without maintaining a centralized system to share and access information.[60]

350. CISA guidance recommends that using a comprehensive network, in addition to network segregation, will help contain the impact of an intrusion and prevent or limit lateral movement on the part of malicious actors.[61]

351. Despite holding the PII and PHI of millions of patients, Defendants failed to adhere to these recommended best practices. Indeed, had Defendants implemented

[58] *Id.* at 5.
[59] *Id.* at 6.
[60] *Id.* at 7-8; *see also* Robert Wood, *Why Data Silos Create Cybersecurity Risks and How to Break Them Down*, ACCELERATION ECONOMY (Feb. 27, 2023), https://accelerationeconomy.com/cybersecurity/why-data-silos-create-cybersecurity-risks-and-how-to-break-them-down/#.
[61] *Id.*

common sense security measures like MFA, the hackers never could have accessed millions of patient files and the Data Breach would have been prevented or much smaller in scope. Defendants also lacked the necessary safeguards to detect and prevent phishing attacks and failed to implement adequate monitoring or control systems to detect the unauthorized infiltration after it occurred.

352. Defendants, like any entity in the healthcare industry their size storing valuable data, should have had robust protections in place to detect and terminate a successful intrusion long before access and exfiltration could expand to millions of patient files. Defendants' below-industry-standard procedures and policies are inexcusable given their knowledge that they were a prime target for cyberattacks.

353. Furthermore, while MFA is critical for preventing data breaches, IT Redundancy helps companies mitigate the effects of a data breach. IT Redundancy means "a provision of duplicate, backup equipment or links that immediately take over the function of equipment or transmission lines that fail."[62] So for example, if a primary server fails, a backup server can takeover, ensuring that patient data is still accessible and that critical healthcare services can continue. Organizations like the American Hospital Association recommend companies in the healthcare industry use "backup technology which renders the backups 'immutable' – unable to be deleted, altered or encrypted."[63]

---

[62] *Redundancy*, GARTNER, https://www.gartner.com/en/information-technology/glossary/redundancy (last visited July 16, 2024).

[63] AHA Cybersecurity Advisory, *UnitedHealth Group's Change Healthcare Experiencing Cyberattack that Could Impact Health Care Providers*, AMERICAN HOSPTIAL ASSOCIATION (Feb. 22, 2024), https://www.aha.org/advisory/2024-02-22-

Unfortunately, like its data security, Change's IT Redundancy is also subpar. As Sen. Wyden emphasized, "[m]ultifactor authentication is vital for prevention, but redundancies . . . help the company get back on its feet . . . [Change] flunked both."[64]

Defendants Failed to Comply with Federal Law and Regulatory Guidance

354. Defendants are covered by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (*see* 45 C.F.R. § 160.102) and as such are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

355. These rules establish national standards for the protection of patient information, including PHI, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. 45 C.F.R. § 160.103.

356. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."[65]

---

unitedhealth-groups-change-healthcare-experiencing-cyberattack-could-impact-health-care-providers-and.

[64] Jessie Hellmann, *UnitedHealth Group CEO blames hack on aged technology systems*, ROLL CALL (May 1, 2024, 5:52 PM), https://rollcall.com/2024/05/01/unitedhealth-group-ceo-blames-hack-on-aged-technology-systems/.

[65] 45 C.F.R. § 164.502.

357. HIPAA requires that Defendants implement appropriate safeguards for this information.[66]

358. HIPAA requires that Defendants provide notice of a breach of unsecured protected health information, which includes protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons—i.e., non-encrypted data.[67]

359. Despite these requirements, Defendants failed to comply with their duties under HIPAA and their own privacy policies. Indeed, Defendants failed to:

(a) Maintain an adequate data security system to reduce the risk of data breaches and cyberattacks;

(b) Adequately protect the PII /PHI of patients;

(c) Ensure the confidentiality and integrity of electronically protected health information created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

(d) Implement technical policies and procedures for electronic information systems that maintain electronically protected health information to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);

(e) Implement adequate policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);

[66] 45 C.F.R. § 164.530(c)(1).
[67] 45 C.F.R. § 164.404; 45 C.F.R. § 164.402.

(f) Implement adequate procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

(g) Protect against 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 C.F.R. § 164.306(a)(3);

(h) Ensure compliance with the electronically protected health information security standard rules by their workforces, in violation of 45 C.F.R. § 164.306(a)(4); and/or

(i) Train all members of their workforces effectively on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of protected health information, in violation of 45 C.F.R. § 164.530(b).

360. Additionally, federal agencies have issued recommendations and guidelines to help minimize the risks of a data breach for businesses holding sensitive data. For example, the Federal Trade Commission (FTC) has issued numerous guides for businesses highlighting the importance of reasonable data security practices, which should be factored into all business-related decision making.[68]

[68] *Start with Security*, FTC, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited July 16, 2024).

361. The FTC's publication Protecting Personal Information: A Guide for Business sets forth fundamental data security principles and practices for businesses to implement and follow as a means to protect sensitive data.[69] Among other things, the guidelines note that businesses should (a) protect the personal customer information that they collect and store; (b) properly dispose of personal information that is no longer needed; (c) encrypt information stored on their computer networks; (d) understand their network's vulnerabilities; and (e) implement policies to correct security problems. The FTC guidelines further recommend that businesses use an intrusion detection system, monitor all incoming traffic for unusual activity, monitor for large amounts of data being transmitted from their system, and have a response plan ready in the event of a breach.[70]

362. Additionally, the FTC recommends that companies limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security; monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[71] This is consistent with guidance provided by the FBI, HHS, and the principles set forth in the CISA 2020 guidance.

363. The FTC has brought enforcement actions against businesses for failing to reasonably protect customer information, treating the failure to employ reasonable and

[69] *Protecting Personal Information*, FTC, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited July 16, 2024).
[70] Id.
[71] *Start with Security*, FTC, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited July 16, 2024).

appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[72]

364. Defendants were fully aware of their obligations to implement and use reasonable measures to protect the PII and PHI of the patients but failed to comply with these basic recommendations and guidelines that would have prevented this Breach from occurring. Defendants' failure to employ reasonable measures to protect against unauthorized access to patient information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

CLASS ACTION ALLEGATIONS

I. NATIONWIDE CLASS

365. Pursuant to Fed. R. Civ. P. 23, Plaintiffs seek certification of the following nationwide class (the "Nationwide Class" or the "Class"):

> Nationwide Class: All healthcare providers whose use of Change's services was disrupted, or whose payments were delayed following the Data Breach announced by UHG in February 2024.

Pursuant to Fed. R. Civ. P. 23, Plaintiffs also seek certification of state-by-state claims in the alternative to the nationwide claims, as well as statutory claims under state data breach statutes and consumer protections statutes, on behalf of separate statewide Classes for each

[72] *Privacy and Security Enforcement*, FTC, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited July 16, 2024).

of the following states: California, Connecticut, Florida, Georgia, Illinois, Iowa, Kansas, Kentucky, Louisiana, Massachusetts, Michigan, Minnesota, Missouri, New Hampshire, New Jersey, North Carolina, Oregon, Pennsylvania, Rhode Island, Texas, Vermont, and Washington (collectively, the "Statewide Classes"), defined as follows:

> [STATE] Class: All healthcare providers residing in [STATE] whose use of Change's services was disrupted, or whose payments were delayed following the Data Breach announced by UHG in February 2024.

The foregoing Statewide Classes, together with the Nationwide Class, are referred to collectively as the "Class" herein. The Statewide Classes, when referred to separately, are each referred to as "[STATE] Class."

366. Excluded from the proposed Class are Defendants, any entity in which Defendants have a controlling interest, is a parent or subsidiary, or which is controlled by Defendants, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendants; and judicial officers to whom this case is assigned and their immediate family members. Also excluded from the Class are any federal, state, or local governmental entities, any judicial officer presiding over this action and the members of their immediate family and judicial staff, and any juror assigned to this action.

367. **Class Identity**: The members of the Class are readily identifiable and ascertainable. Defendants and/or their affiliates, among others, possess the information to identify and contact Class members.

368. **Numerosity**: The members of the Class are so numerous that joinder of all of them is impracticable. According to the U.S. Department of Health and Human Services,

Change "processes 15 billion health care transactions annually and is involved in one in every three patient records." According to Change, it is connected to "more than 800,000 providers[.]"

369. **Typicality**: Plaintiffs' claims are typical of the claims of the members of the Class because all Class members could not submit medical claims through Defendants' Change Platform or were delayed payment following the Data Breach and were harmed as a result.

370. **Adequacy**: Plaintiffs will fairly and adequately protect the interests of the Class. Plaintiffs have no known interests antagonistic to those of the Class and their interests are aligned with Class members' interests. Plaintiffs could not submit medical claims through Defendants' Change Platform and/or their payments were delayed following the Data Breach just as Class members' were, and suffered similar harms. Plaintiffs have also retained competent counsel with significant experience litigating complex and commercial class actions.

371. **Commonality and Predominance**: There are questions of law and fact common to the Class such that there is a well-defined community of interest in this litigation. These common questions predominate over any questions affecting only individual Class members. The common questions of law and fact include, without limitation:

(a) Whether Defendants owed Plaintiffs and Class members a duty to implement and maintain reasonable security procedures and practices to protect patients' PII and PHI;

(b) Whether Defendants received a benefit without proper restitution making it unjust for Defendants to retain the benefit without commensurate compensation;

(c) Whether Defendants acted negligently by not implementing adequate security systems to ensure their network was not disconnected;

(d) Whether Defendants violated their duty to implement adequate security systems to ensure their network was not disconnected;

(e) Whether Defendants' breaches of their duties to implement reasonable security systems directly and/or proximately caused damages to Plaintiffs and Class members;

(f) Whether Defendants adequately addressed and fixed the vulnerabilities that enabled the Data Breach;

(g) Whether Defendants breached agreements with Plaintiffs and Class members by disconnecting the Change Platform; and

(h) Whether Class members are entitled to compensatory damages, punitive damages, and/or statutory or civil penalties as a result of the Data Breach.

372. Defendants have engaged in a common course of conduct and Plaintiffs and Class members have been similarly impacted by Defendants' failure to maintain reasonable security procedures and practices to protect patients' PII and PHI.

373. **Superiority**: A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class

action, most if not all Class members would find the cost of litigating their individual claims prohibitively high and have no effective remedy. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members and risk inconsistent treatment of claims arising from the same set of facts and occurrences. Plaintiffs know of no difficulty likely to be encountered in the maintenance of this action as a class action under the applicable rules.

CLAIMS FOR RELIEF

COUNT I
Negligence
(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, the Statewide Classes)

374. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

375. Defendants owed Plaintiffs and Class members a duty to act with reasonable care to maintain a secure network and ensure that Change's claims processing and revenue and payment cycle management services would be properly functioning, timely, and accurate. Defendants used their computer networks to ensure that claims were being processed and accurate payments were being distributed to Plaintiffs and Class members.

376. Defendants also owed Plaintiffs and Class members a duty to not cause harm to Plaintiffs and Class members because they were foreseeable and probable victims of substandard cybersecurity practices, such as a lack of MFA. Because if Defendants' network was not secure and susceptible to breach, then the network that houses Change's

claims processing and payment cycle services would be disconnected and Plaintiffs and Class members would be injured as described herein without use of Defendants' services and the Change Platform.

377. Defendants knew or should have known of the vulnerabilities of their cybersecurity systems and the significance of adequate security measures. Defendants knew or should have known about the prevalence of data breaches in the healthcare sector. And Defendants knew or should have known that their network security did not adequately safeguard the claims processing and payment cycle services.

378. Defendants' duty to use reasonable care in securing their networks so as to protect against disconnection of the Change Platform is a result of the parties' relationship, as well as common law and federal law, and Defendants' own policies and promises regarding privacy and data security.

379. Defendants breached their duties to Plaintiffs and Class members in numerous ways, as described herein, including by:

(a) Failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the Change Platform;

(b) Failing to comply with industry standard data security measures for the healthcare industry leading up to the Data Breach;

(c) Failing to comply with their own privacy and data security policies; and

(d) Failing to adequately monitor, evaluate, and ensure the security of their network and systems.

380. Plaintiffs and Class members would have been able to timely submit medical claims and receive timely payment but for Defendants' wrongful and negligent breaches of their duties.

381. Defendants knew that a breach of their systems could injure healthcare providers who use and rely on the Change Platform to timely process medical claims and receive timely payment.

382. Plaintiffs' and Class members' decision to trust Defendants with their processing needs was based on Defendants' statements and assurances that Defendants would take adequate security precautions and maintain industry standard cybersecurity measures, such as MFA.

383. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class members have suffered damages as discussed herein, including missed payments and out-of-pocket expenses associated with (i) purchasing new healthcare payment software; (ii) notifying patients of the Data Breach; and (iii) late penalties assessed for untimely payment of expenses. Furthermore, Plaintiffs' and Class members' damages include time and effort spent researching and implementing new healthcare payment software. Plaintiffs and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and have incurred extra costs from switching to another healthcare payment software.

COUNT II
Negligence Per Se
(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, the Statewide Classes)

384. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

385. Defendants' duties arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including as interpreted by the FTC, the unfair act or practice by a business, such as Defendants, of failing to employ reasonable security measures to ensure access to their paid-for Change Platform, despite representing otherwise.

386. Defendants have additional duties under the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules"), which require, *inter alia*, that Defendants maintain adequate data security systems to reduce the risk of data breaches and cyberattacks, adequately protect the PHI of patients, and ensure the confidentiality and integrity of electronically protected health information created, received, maintained, or transmitted. *See, e.g.*, 45 C.F.R. § 164.306(a)(1).

387. Defendants violated Section 5 of the FTCA and HIPAA Privacy and Security Rules by failing to use reasonable security measures to ensure access to their paid-for Change Platform, despite representing otherwise, by not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of sensitive information they collect, maintain, and/or transfer as well as the nature of their businesses. Defendants' conduct was also unreasonable given the

foreseeable consequences of a data breach where Defendants disconnect the network and the Change Platform would cause substantial damages to Plaintiffs and Class members.

388. Defendants' violation of Section 5 of the FTCA and HIPAA Privacy and Security Rules constitutes negligence per se.

389. Plaintiffs and Class members are within the class of persons that Section 5 of the FTCA and HIPAA Privacy and Security Rules were intended to protect.

390. The harm occurring as a result of the Data Breach is the type of harm that Section 5 of the FTCA and HIPAA Privacy and Security Rules were intended to guard against. The FTC has pursued enforcement actions against businesses, which as a result of their failure to employ reasonable data security measures and avoid unfair practices or deceptive practices, caused the same type of harm that has been suffered by Plaintiffs and Class members as a result of the Data Breach.

391. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in securing their networks that provide access to the Change Platform would result in Plaintiffs and Class members failing to receive timely payments and inhibit their ability to submit medical claims.

392. The injury and harm that Plaintiffs and the other Class members suffered was the direct and proximate result of Defendants' violation of Section 5 of FTCA and HIPAA Privacy and Security Rules. Plaintiffs and Class members have suffered damages as discussed herein, including missed payments and out-of-pocket expenses associated with (i) purchasing new healthcare payment software/services; (ii) notifying patients of Data Breach; and (iii) late penalties assessed for untimely payment of expenses. Furthermore,

Plaintiffs' and Class members' damages include time and effort spent researching and implementing new healthcare payment software and services, hiring staff or third-party companies to troubleshoot the business disruption caused by Defendants' shutdown of the Change Platform, obtaining loans or funds—including application fees and interest—to fund operations that they would not have otherwise been obligated to obtain had Defendants timely processed and paid their insurance claims. Plaintiffs and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and have incurred extra costs from switching to another healthcare payment software.

COUNT III
Breach of Express Contract
(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, the Statewide Classes)

393. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

394. Acting in the ordinary course of business, Defendants contract with healthcare providers (such as Plaintiffs and Class members) directly, or with third-party companies who provide services to healthcare providers (such as Plaintiffs and Class members) using Defendants' services and the Change Platform, to provide healthcare insurance—and related services for processing and paying insurance claims for same—to patients. Through the regular, ordinary course of their business in providing those services, Defendants obtain patients' PII and PHI directly from healthcare providers (such as Plaintiffs and Class members) who use Defendants' services and the Change Platform, or

indirectly through those third-party intermediaries who use Defendants' services and the Change Platform to provide insurance claims processing services to healthcare providers (such as Plaintiffs and Class members).

395. Each of those respective contracts between Defendants and healthcare providers (such as Plaintiffs and Class members) or between Defendants and third-party intermediaries who use Defendants' services and the Change Platform to provide insurance claims processing services to healthcare providers (such as Plaintiffs and Class members) contain provisions requiring Defendants to protect the sensitive PII and PHI that Defendants receive in order to provide such insurance functions—directly or indirectly—to Plaintiffs and Class members.

396. To the extent that Plaintiffs and Class members contract directly with Defendants for their services, Defendants breached these provisions in those contracts by failing to safeguard sensitive information entrusted to them and allowing the Data Breach to occur.

397. Further, with respect to Plaintiffs and Class members who do not directly contract with Defendants, these provisions requiring that Defendants—acting in the ordinary course of business—protect the PII and PHI of Plaintiffs' and Class members' patients were intentionally included in Defendants' contracts with the third-party intermediaries for the direct benefit of Plaintiffs and Class members, such that Plaintiffs and Class members are intended third party beneficiaries of Defendants' contracts, and therefore entitled to enforce them.

398. Defendants breached these contracts while acting in the ordinary course of business by not protecting the PII and PHI of Plaintiffs' and Class members' patients, as alleged in depth herein.

399. As a direct and proximate result of Defendants' breaches, Plaintiffs and Class members sustained actual losses and damages alleged in detail herein. Plaintiffs and Class members alternatively seek an award of nominal damages.

400. Further, these contracts were subject to implied covenants of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform their contractual obligations (both explicit and fairly implied) and not to impair the rights of the other parties to receive the rights, benefits, and reasonable expectations under the contracts. These included the implied covenants that Defendants would act fairly and in good faith in carrying out their contractual obligations to take reasonable measures to protect Plaintiffs' and Class members' PII and PHI and to comply with industry standards and federal and state laws and regulations.

401. A "special relationship" exists between Defendants and the Plaintiffs and Class members. Defendants entered into a "special relationship" with Plaintiffs and Class members who use Defendants' services and the Change Platform—either directly or indirectly through third party intermediaries that use those services on Plaintiffs' and Class members' behalf—and, in doing so, entrusted Defendants with their patients' sensitive PII and PHI while using Defendants' services and the Change Platform to process health insurance claims.

402. Despite this special relationship with Plaintiffs and Class members, Defendants did not act in good faith and with fair dealing to protect Plaintiffs' and Class members' PII and PHI.

403. Plaintiffs and Class members performed all conditions, covenants, obligations, and promises owed to Defendants.

404. Defendants' failure to act in good faith in implementing the security measures required by the contracts denied Plaintiffs and Class members the full benefit of their bargain, and instead they received health insurance claims processing and related services that were less valuable than what they paid for and less valuable than their reasonable expectations under the contracts. Plaintiffs and Class members were damaged in an amount at least equal to this overpayment. Defendants' failure to act in good faith in implementing the security measures required by the contracts also caused Plaintiffs and Class members to suffer actual damages resulting from the theft of their PII and PHI and remain at imminent risk of suffering additional damages in the future. Accordingly, Plaintiffs and Class members have been injured as a result of Defendants' breach of the covenant of good faith and fair dealing and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT IV
Breach of Implied Contract
(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, the Statewide Classes)

405. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

406. Plaintiffs and Class members were required to provide their patients' PII and PHI to Defendants as a condition of receiving services from Defendants and/or third-party intermediaries using Defendants' services on behalf of Plaintiffs and Class members.

407. Plaintiffs and Class members entrusted their patients' PII and PHI to Defendants. In so doing, Plaintiffs and Class members entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and Class members if their data had been breached and compromised or stolen.

408. Implicit in the agreement between Plaintiffs, Class members, and the Defendants regarding the provision of PII and PHI, which Plaintiff and Class members were required to provide to Defendants, were the following obligations for the Defendants: (a) restrict the use of such PII and PHI solely for business purposes, (b) implement reasonable measures to safeguard the PII and PHI, (c) prevent unauthorized disclosures of the PII and PHI, (d) promptly and adequately notify Plaintiff and Class members of any unauthorized access and/or theft of their PII and PHI, (e) reasonably safeguard and protect the PII and PHI of Plaintiffs' and Class members' patients from unauthorized disclosure or use, and (f) maintain the PII and PHI under conditions ensuring their security and confidentiality.

409. The mutual understanding and intent between Plaintiffs, Class members, and Defendants are evident through their conduct and ongoing business interactions.

410. Defendants solicited, offered, and invited Plaintiffs and Class members to provide their patients' PII and PHI as part of Defendants' regular business practices.

Plaintiffs and Class members accepted Defendants' offers and provided their patients' PII and PHI to Defendants.

411. In accepting the PII and PHI of Plaintiffs and Class members, Defendants understood and agreed that they were required to reasonably safeguard the PII and PHI from unauthorized access or disclosure.

412. At all relevant times Defendants promulgated, adopted, and implemented written privacy policies whereby they expressly promised Plaintiffs and Class members that they would only disclose PII and PHI under certain circumstances, none of which relate to the Data Breach.

413. Defendants further promised to comply with industry standards and to make sure that Plaintiffs' and Class members' PII and PHI would remain protected.

414. When entering into these implied contracts, Plaintiffs and Class members reasonably believed and anticipated that Defendants' data security practices adhered to pertinent laws and regulations and aligned with industry standards.

415. Plaintiffs and Class members paid money to Defendants with the reasonable belief and expectation that Defendants would use part of their earnings to obtain adequate data security. Defendants failed to do so.

416. Plaintiffs and Class members would not have entrusted their patients' PII and PHI to Defendants in the absence of the implied contract between them and Defendants to keep that information reasonably secure.

417. Plaintiffs and Class members would not have entrusted their patients' PII and PHI to Defendants in the absence of their implied promise to monitor their computer systems and networks to ensure that they adopted reasonable data security measures.

418. Plaintiffs and Class members fully and adequately performed their obligations under the implied contracts with Defendants.

419. Defendants breached the implied contracts they made with Plaintiffs and Class members by failing to safeguard and protect their personal information, by failing to delete the PII and PHI of Plaintiffs' and Class members' patients once the relationship ended, and by failing to provide accurate notice to them that PII and PHI was compromised as a result of the Data Breach.

420. As a direct and proximate result of Defendants' breach of the implied contracts, Plaintiffs and Class members sustained damages, as alleged herein, including the loss of the benefit of the bargain.

421. Plaintiffs and Class members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

COUNT V
Unjust Enrichment
(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, the Statewide Classes)

422. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

423. This Count is pleaded in the alternative to Plaintiffs' breach of express and implied contract claims above (Counts III and IV).

424. Plaintiffs and Class members conferred benefits on Defendants, both directly and indirectly, in the form of payments for claims management and processing, insurance verification, authorization and medical necessity reviews, provision of services to Defendants' insureds prior to payment, provision of services to insureds of Defendants' insurer customers who use the Change Platform to process claims, and disbursement of payments, among other things. Defendants had knowledge of the benefits conferred by Plaintiffs and Class members and appreciated, and retained, such benefits. In accepting PII and PHI and money from Plaintiffs and Class members, Defendants should have used, in part, the monies Plaintiffs and Class members paid to them, directly and indirectly, to pay the costs of basic industry standard cybersecurity, threat detection, and incident response measures, including a business continuity plan. In failing to provide such measures, the Defendants have been unjustly enriched at Plaintiffs' and Class Members' expense. Defendants had no justification for failing to provide adequate security protections.

425. Plaintiffs and Class members have suffered actual damages and harm because of Defendants' negligent, and unlawful, conduct, inactions, and omissions. Defendants should be required to disgorge into a common fund for the benefit of Plaintiffs and Class members all unlawful or inequitable proceeds received from Plaintiffs and Class members.

COUNT VI
Negligent Interference with Prospective Economic Advantage
(On Behalf of Plaintiffs and the Nationwide Class, or, Alternatively, the Statewide Classes)

426. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

427. Plaintiffs and Class members had an ongoing business relationship with third party businesses, including practice management companies, that would have likely resulted in future economic benefits to Plaintiffs and Class members. Defendants knew or should have known about Plaintiffs' and Class members' relationships with third party businesses due to the integration of Change's services and processes with such third parties.

428. The harm to Plaintiffs and the Class members resulting from the Data Breach and network outage was foreseeable.

429. Defendants failed to act with reasonable care and engaged in wrongful conduct, including by violating Section 5 of FTCA and HIPAA Privacy and Security Rules.

430. The relationship between Plaintiffs and Class members and the third-party businesses was disrupted, resulting in economic harm to Plaintiffs and Class members.

431. Defendants' wrongful conduct was a substantial factor in causing the harm to Plaintiffs and the Class. As a direct and proximate cause, Plaintiffs and Class members have suffered damages as discussed herein, including missed payments and out-of-pocket expenses associated with (i) purchasing new healthcare payment software/services; (ii) notifying patients of the Data Breach; and (iii) late penalties assessed for untimely payment of expenses. Furthermore, Plaintiffs' and Class members' damages include time and effort spent researching and implementing new healthcare payment software and services, hiring staff or third-party companies to troubleshoot the business disruption caused by Defendants' shutdown of the Change Platform, obtaining loans or funds—including

application fees and interest—to fund operations that they would not have otherwise been obligated to obtain had their insurance claims been timely processed and paid by Defendants. Plaintiffs and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and have incurred extra costs from switching to another healthcare payment software.

COUNT VII
Violation of California's Unfair Competition Law,
Cal. Bus. & Prof. Code §§ 17200, *et seq.*
(On Behalf of Plaintiffs Parker, ShaMynds, and the Nationwide Class, or Alternatively, the California Class)

432. Plaintiffs Parker and ShaMynds Healing Center, PC repeat and reallege every allegation set forth in the preceding paragraphs.

433. Defendants are "person[s]" as defined by Cal. Bus. & Prof. Code § 17201.

434. Defendants violated Cal. Bus. & Prof. Code §§ 17200, *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

435. As set forth herein, Defendants engaged in unfair and deceptive acts or practices, including but not limited to:

(a) Failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect the network that powers the Change Platform despite representation otherwise;

(b) Failing to comply with common law and statutory duties pertaining to the security of the network that powers the Change Platform, including duties imposed by Section 5 of the FTCA and HIPAA Privacy and Security Rules;

(c) Failing to properly protect the integrity of the systems powering the Change Platform;

(d) Misrepresenting that Defendants maintained reasonable and adequate security measures;

(e) Misrepresenting that Defendants would comply with common law and statutory duties pertaining to security of their network, including duties imposed by Section 5 of the FTCA and HIPAA Privacy and Security Rules;

(f) Omitting, suppressing, and concealing the material fact that Defendants did not properly secure their systems powering the Change Platform;

(g) Omitting, suppressing, and concealing the material fact that Defendants did not comply with common law and statutory duties pertaining to the security of their network, including duties imposed by Section 5 of the FTCA and HIPAA Privacy and Security Rules; and

(h) Overcharging for services provided without adequate security measures in place.

436. Defendants engaged in unlawful business practices by violating Cal. Civ. Code § 1798.82.

437. Defendants knowingly and willingly represented that their network maintained adequate protections to induce Plaintiffs Parker, ShaMynds, and the California Class to use and rely on Change's services.

438. Defendants' concealments, omissions, and false promises induced Plaintiffs Parker, ShaMynds and the California Class to use and rely on Change's services. But for these unlawful acts by Defendants, Plaintiffs Parker, ShaMynds, and the California Class would not have used or relied on Defendants' services.

439. Defendants engaged in unfair or deceptive action in violation of the UCL by failing to implement and maintain reasonable security measures to ensure continued access to the Change Platform in a manner that complied with applicable laws, regulations, and industry standards, and Defendants represented they would.

440. As a direct and proximate result of Defendants' conduct alleged herein and violation of the UCL, Plaintiffs and Class members have suffered damages as discussed herein, including missed payments and out-of-pocket expenses associated with (i) purchasing new healthcare payment software/services; (ii) notifying patients of the Data Breach; and (iii) late penalties assessed for untimely payment of expenses. Furthermore, Plaintiffs and Class members' damages include time and effort spent researching and implementing new healthcare payment software and services, hiring staff or third-party companies to troubleshoot the business disruption caused by Defendants' shutdown of the Change Platform, obtaining loans or funds—including application fees and interest—to fund operations that they would not have otherwise been obligated to obtain had Defendants timely processed and paid their insurance claims. Plaintiffs and Class members

have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and have incurred extra costs from switching to another healthcare payment software.

COUNT VIII
Violation of the Connecticut Unfair Trade Practices Act,
Conn. Gen. Stat. §§ 42-110, *et seq.*
(On Behalf of Plaintiffs Authentic Living, Killingly, and the Nationwide Class, or, Alternatively, the Connecticut Class)

441. Plaintiffs Authentic Living, Killingly, and the Connecticut Class repeat and reallege every allegation set forth in the preceding paragraphs.

442. Plaintiffs Authentic Living, Killingly, and the Connecticut Class are "person[s]" within the meaning of the Connecticut Unfair Trade Practices Act ("CUTPA"), Conn. Gen. Stat. § 42-110a(3).

443. Defendants conducted business in Connecticut for purposes of this claim. Class members transacted with Defendants in Connecticut, and Class members were deceived in Connecticut when they were not informed of Defendants' deficient data security practices.

444. The CUTPA states: "No person shall engage in unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade prohibits unfair methods of competition and unfair practices in the conduct of trade or commerce." Conn. Gen. Stat. § 42-110a.

445. Defendants advertised, offered, or sold services in Connecticut and engaged in trade or commerce directly or indirectly affecting Plaintiffs Authentic Living and Killingly under Conn. Gen. Stat. § 42-110a (4).

446. Defendants engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce under Conn. Gen. Stat. § 42-110a, including:

(a) Representing that their goods and services have characteristics, uses, and benefits that they do not have; and

(b) Representing that their goods and services are of a particular standard or quality if they are of another.

447. Defendants' unfair, unconscionable, and deceptive practice include but are not limited to:

(a) Failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect the network that powers the Change Platform despite representation otherwise;

(b) Failing to comply with common law and statutory duties pertaining to the security of the network that powers the Change Platform, including duties imposed by Section 5 of the FTCA and HIPAA Privacy and Security Rules;

(c) Failing to properly protect the integrity of the systems powering the Change Platform;

(d) Misrepresenting that Defendants maintained reasonable and adequate security measures;

(e) Misrepresenting that Defendants would comply with common law and statutory duties pertaining to security of the network, including duties imposed by Section 5 of the FTCA;

(f) Omitting, suppressing, and concealing the material fact that Defendants did not employ reasonable measures to secure the Change Platform;

(g) Omitting, suppressing, and concealing the material fact that Defendants did not comply with common law and statutory duties pertaining to the security of their network, including duties imposed by Section 5 of the FTCA and HIPAA Privacy and Security Rules; and

(h) Overcharging for services provided without adequate security measures in place.

448. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and the ability to ensure access to the Change Platform.

449. Defendants knowingly and willingly represented that their network maintained adequate protections to induce Plaintiffs Authentic Living, Killingly, and the Connecticut Class to use and rely on Defendants' services.

450. Defendants' concealments, omissions, and false promises induced Plaintiffs Authentic Living, Killingly, and the Connecticut Class to use and rely on Defendants' services. But for these unlawful acts by Defendants, Plaintiffs Authentic Living, Killingly, and the Connecticut Class would not have used or relied on Defendants' services, or would have paid less for them, had they known of Defendants' inadequate security practices.

Defendants could and should have made a proper disclosure to inform consumers of the inadequate data security when Plaintiffs transacted with Defendants.

451. The CUTPA states: "Any person who suffers any ascertainable loss of money or property, real or personal, as a result of the use or employment of a method, act, or practice prohibited by section 42-110b, may bring an action . . . to recover actual damages. . . . The court may, in its discretion, award punitive damages and may provide such equitable relief as it deems necessary or property."

452. As a direct and proximate result of Defendants' conduct alleged herein and in violation of the CUTPA, Plaintiffs and Class members have suffered an "ascertainable loss of money or property" as discussed herein, including missed payments and out-of-pocket expenses associated with (i) purchasing new healthcare payment software/services; (ii) notifying patients of the Data Breach; and (iii) late penalties assessed for untimely payment of expenses. Furthermore, Plaintiffs and Class members' damages include time and effort spent researching and implementing new healthcare payment software and services, hiring staff or third-party companies to troubleshoot the business disruption caused by Defendants' shutdown of the Change Platform, obtaining loans or funds—including application fees and interest—to fund operations that they would not have otherwise been obligated to obtain had Defendants timely process and paid their insurance claims. Plaintiffs and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and have incurred extra costs from switching to another healthcare payment software.

453. Plaintiffs and Class members suffered "actual damages" based on the various types of damages alleged herein.

454. Plaintiffs are entitled to punitive damages under Conn. Gen. Stat. § 42-110g(a). Defendants knew or should have known that their data security practices were deficient. Among other things, Defendants should have known that the healthcare industry was a frequent target of sophisticated cyberattacks. Defendants knew or should have known that their data security was insufficient to guard against those attacks.

455. Plaintiffs and Class members are entitled to recovery of their costs and reasonable attorneys' fees under Conn. Gen. Stat. § 42-110g(d).

COUNT IX
Violation of the Illinois Consumer Fraud and Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 505/1(c)
(On Behalf of Plaintiff Balance Fitness for Life and the Nationwide Class, or, Alternatively, the Illinois Class)

456. Plaintiff Balance Fitness for Life and the Illinois Class repeat and reallege every allegation set forth in the preceding paragraphs.

457. Plaintiff Balance Fitness for Life and the Illinois Class are "person[s]" within the meaning of the Illinois Consumer Fraud and Deceptive Trade Practices Act ("ICFDTPA"), 815 Ill. Comp. Stat.§ 505/1(c).

458. Defendants advertised, offered, or sold services in Illinois and engaged in trade or commerce directly or indirectly affecting Plaintiff Balance Fitness for Life under 815 Ill. Comp. Stat. § 505/1(f).

459. The Illinois Consumer Fraud and Deceptive Business Practices Act (ICFDBA) prohibits unfair methods of competition and unfair practices in the conduct of trade or commerce under 815 Ill. Comp. Stat. § 505/2.

460. Defendants engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce under 815 Ill. Comp. Stat. § 505/2, including:

(a) Representing that their goods and services have characteristics, uses, and benefits that they do not have; and

(b) Representing that their goods and services are of a particular standard or quality if they are of another.

461. Defendants' unfair, unconscionable, and deceptive practice include but are not limited to:

(a) Failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect the network that powers the Change Platform despite representation otherwise;

(b) Failing to comply with common law and statutory duties pertaining to the security of the network that powers the Change Platform, including duties imposed by Section 5 of the FTCA and HIPAA Privacy and Security Rules.

(c) Failing to properly protect the integrity of the systems powering the Change Platform;

(d) Misrepresenting that Defendants maintained reasonable and adequate security measures;

(e) Misrepresenting that Defendants would comply with common law and statutory duties pertaining to security of the network, including duties imposed by Section 5 of the FTCA;

(f) Omitting, suppressing, and concealing the material fact that Defendants did not properly secure their systems powering the Change Platform;

(g) Omitting, suppressing, and concealing the material fact that Defendants did not comply with common law and statutory duties pertaining to the security of their network, including duties imposed by Section 5 of the FTCA and HIPAA Privacy and Security Rules; and

(h) Overcharging for services provided without adequate security measures in place.

462. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and the ability to ensure access to the Change Platform.

463. Defendants knowingly and willingly represented that their network maintained adequate protections to induce Plaintiff Balance Fitness for Life and the Illinois Class to use and rely on Defendants' services.

464. Defendants' concealments, omissions, and false promises induced Plaintiff Balance Fitness for Life and the Illinois Class to use and rely on Defendants' services. But for these unlawful acts by Defendants, Plaintiff Balance Fitness for Life and the Illinois

Class would not have used or relied on Defendants' services or would have paid less for them.

465. As a direct and proximate result of Defendants' conduct alleged herein and in violation of the ICFDTPA and ICFDBA, Plaintiffs and Class members have suffered damages as discussed herein, including (i) purchasing new healthcare payment software/services; (ii) notifying patients of the Data Breach; and (iii) late penalties assessed for untimely payment of expenses. Furthermore, Plaintiffs and Class members' damages include time and effort spent researching and implementing new healthcare payment software and services, hiring staff or third-party companies to troubleshoot the business disruption caused by Defendants' shutdown of the Change Platform, obtaining loans or funds—including application fees and interest—to fund operations that they would not have otherwise been obligated to obtain had Defendants timely process and paid their insurance claims. Plaintiffs and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and have incurred extra costs from switching to another healthcare payment software.

COUNT X
Violation of New Hampshire's Regulation of Business Practices for Consumer Protection, N.H. Rev. Stat. Ann. §§ 358-A, *et seq.*
(On Behalf of Plaintiff HealthFirst and the Nationwide Class, or, Alternatively, the New Hampshire Class)

466. Plaintiff HealthFirst, and the New Hampshire Class repeat and reallege every allegation set forth in the preceding paragraphs.

467. Plaintiff HealthFirst, the New Hampshire Class, and Defendants are "persons" as defined by N.H. Rev. Stat. Ann. § 358-A:1.

468. Defendants advertised, offered, or sold services in New Hampshire and engaged in trade or commerce directly or indirectly affecting Plaintiff HealthFirst, and the New Hampshire Class as defined by N.H. Rev. Stat. Ann. § 358-A:2.

469. The Regulation of Business Practices for Consumer Protection (the "New Hampshire Consumer Protection Act") prohibits any person from using "any unfair method of competition or any unfair or deceptive act or practice in the conduct of any trade or commerce within this state." N.H. Rev. Stat. Ann. 358-A:2.

470. Defendants engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of N.H. Rev. Stat. Ann. § 358-A.2, including:

(a) Representing that their goods and services have characteristics, uses, and benefits that they do not have, in violation of N.H. Rev. Stat. Ann. § 358-A:2(V); and

(b) Representing that their goods and services are of a particular standard or quality if they are of another in violation of N.H. Rev. Stat. Ann. § 358-A:2(VII).

471. Defendants' unfair, unconscionable, and deceptive practices include but are not limited to:

(a) Failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and

protect their network that powers the Change Platform despite representation otherwise;

(b) Failing to comply with common law and statutory duties pertaining to the security of their network that powers the Change Platform, including duties imposed by Section 5 of the FTCA and HIPAA Privacy and Security Rules;

(c) Failing to properly protect the integrity of the systems powering the Change Platform;

(d) Misrepresenting that Defendants maintained reasonable and adequate security measures;

(e) Misrepresenting that Defendants would comply with common law and statutory duties pertaining to security of their network, including duties imposed by Section 5 of the FTCA;

(f) Omitting, suppressing, and concealing the material fact that Defendants did not properly secure their systems powering the Change Platform;

(g) Omitting, suppressing, and concealing the material fact that Defendants did not comply with common law and statutory duties pertaining to the security of their network, including duties imposed by Section 5 of the FTCA.

(h) Overcharging for services provided without adequate security measures in place.

472. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and the ability to ensure access to the Change Platform.

473. Defendants knowingly and willingly represented that their network maintained adequate protections to induce Plaintiff HealthFirst, and the New Hampshire Class to use and rely on Change's services.

474. Defendants' concealments, omissions, and false promises induced Plaintiff HealthFirst, and the New Hampshire Class to use and rely on Defendants' services. But for these unlawful acts by Defendants, Plaintiff HealthFirst, and the New Hampshire Class would not have used or relied on Defendants' services.

475. As a direct and proximate result of Defendants' conduct alleged herein and in violation of the New Hampshire Consumer Protection Act, Plaintiffs and Class members have suffered damages as discussed herein, including missed payments and out-of-pocket expenses associated with missed payments and out-of-pocket expenses associated with (i) purchasing new healthcare payment software/services; (ii) notifying patients of the Data Breach; and (iii) late penalties assessed for untimely payment of expenses. Furthermore, Plaintiffs and Class members' damages include time and effort spent researching and implementing new healthcare payment software and services, hiring staff or third-party companies to troubleshoot the business disruption caused by Defendants' shutdown of the Change Platform, obtaining loans or funds—including application fees and interest—to fund operations that they would not have otherwise been obligated to obtain had Defendants timely process and paid their insurance claims. Plaintiffs and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and have incurred extra costs from switching to another healthcare payment software.

COUNT XI
Violation of the New Jersey Consumer Fraud Act, N.J. Stat. §§ 56:8-1, *et seq.*
(On Behalf of Plaintiff LDK and the Nationwide Class, or, Alternatively, the New Jersey Class)

476. Plaintiff LDK and the New Jersey Class repeat and reallege every allegation set forth in the preceding paragraphs.

477. Plaintiff LDK and the New Jersey Class are "persons" as defined within N.J. Stat. § 56:8-1(d).

478. Defendants advertised, offered, or sold services in New Jersey and engaged in trade or commerce directly or indirectly affecting Plaintiff LDK.

479. The New Jersey Consumer Fraud Act (NJCFA) prohibits unfair methods of competition and unfair practices in the conduct of trade or commerce and protects consumers against "any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise . . . " N.J. Stat. § 56:8-2.

480. Defendants engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce under N.J. Stat. § 56:8-2, including:

(a) Representing that their goods and services have characteristics, uses, and benefits that they do not have; and

(b) Representing that their goods and services are of a particular standard or quality if they are of another.

481. Defendants' unfair, unconscionable, and deceptive practice include but are not limited to:

(a) Failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect the network that powers the Change Platform despite representation otherwise;

(b) Failing to comply with common law and statutory duties pertaining to the security of their network that powers the Change Platform, including duties imposed by Section 5 of the FTCA and HIPAA Privacy and Security Rules;

(c) Failing to properly protect the integrity of the systems powering the Change Platform;

(d) Misrepresenting that Defendants maintained reasonable and adequate security measures;

(e) Misrepresenting that Defendants would comply with common law and statutory duties pertaining to security of their network, including duties imposed by Section 5 of the FTCA and HIPAA Privacy and Security Rules;

(f) Omitting, suppressing, and concealing the material fact that Defendants did not properly secure their systems powering the Change Platform;

(g) Omitting, suppressing, and concealing the material fact that Defendants did not comply with common law and statutory duties pertaining to the security

of their network, including duties imposed by Section 5 of the FTCA and HIPAA Privacy and Security Rules; and

(h) Overcharging for services provided without adequate security measures in place.

482. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and the ability to ensure access to the Change Platform.

483. Defendants knowingly and willingly represented that their network maintained adequate protections to induce Plaintiff LDK and the New Jersey Class to use and rely on Defendants' services.

484. Defendants' concealments, omissions, and false promises inducted Plaintiff LDK and the New Jersey Class to use and rely on Defendants' services. But for these unlawful acts by Defendants, Plaintiff LDK and the New Jersey Class would not have used or relied on Defendants' services or would have paid less for Defendants' services.

485. As a direct and proximate result of Defendants' conducts alleged herein and in violation of the NJCFA, Plaintiffs and Class members have suffered ascertainable loss and damages as discussed herein, including missed payments and out-of-pocket expenses associated with missed payments and out-of-pocket expenses associated with (i) purchasing new healthcare payment software/services; (ii) notifying patients of the Data Breach; and (iii) late penalties assessed for untimely payment of expenses. Furthermore, Plaintiffs and Class members' damages include time and effort spent researching and implementing new healthcare payment software and services, hiring staff or third-party

companies to troubleshoot the business disruption caused by Defendants' shutdown of the Change Platform, obtaining loans or funds—including application fees and interest—to fund operations that they would not have otherwise been obligated to obtain had Defendants timely process and paid their insurance claims. Plaintiffs and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and have incurred extra costs from switching to another healthcare payment software.

COUNT XII
Violation of the Tennessee Consumer Protection Act,
Tenn. Code Ann. § § 47-18-101, *et seq.*
(On Behalf of Plaintiffs and the Nationwide Class)

486. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

487. Plaintiffs, Class members, and Defendants are each a "person" within the meaning of the Tennessee Consumer Protection Act ("TCPA"). § 47-18-103(14).

488. At all relevant times, Defendants were willfully and knowingly engaged in the use of an unfair and deceptive practice declared to be unlawful.

489. Under the TCPA, it is an unfair or deceptive act to represent that services are of a particular standard and quality if they are not. § 47-18-104(b)(7). It is also unlawful under the TCPA to represent that services have certain characteristics that they do not have. § 47-18-104(b)(5).

490. As set forth herein, Defendants engaged in unfair and deceptive acts or practices, including but not limited to:

(a) Failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect its network that powers the Change Platform despite representation otherwise.

(b) Failing to comply with common law and statutory duties pertaining to the security of its network that powers the Change Platform, including duties imposed by the Section 5 of the FTCA and HIPAA Privacy and Security Rules.

(c) Failing to properly protect the integrity of the systems powering the Change Platform;

(d) Misrepresenting that Change maintained reasonably and adequate security measures;

(e) Misrepresenting that Change would comply with common law and statutory duties pertaining to security of its network, including duties imposed by Section 5 of the FTCA and HIPAA Privacy and Security Rules;

(f) Omitting, suppressing, and concealing the material fact that Change did not properly secure its system power the Change Platform;

(g) Omitting, suppressing, and concealing the material fact that Defendants did not comply with common law and statutory duties pertaining to the security of its network, including duties imposed by Section 5 of the FTCA and HIPAA Privacy and Security Rules.

(h) Overcharging for services provided without adequate security measures in place.

491. Defendants knowingly and willingly represented that their network maintained adequate protections to induce Plaintiffs and Class members to use and rely on Defendants' services.

492. Defendants' concealments, omissions, and false promises induced Plaintiffs and Class members to use and rely on Defendants' services. But for these unlawful acts by Defendants, Plaintiffs and Class members would not have used or relied on Defendants' services.

493. Defendants engaged in unfair or deceptive action in violation of the TCPA by failing to implement and maintain reasonable security measures to ensure continued access to the Change Platform in a manner that complied with applicable laws, regulations, and industry standards, and Defendants represented they would.

494. As a direct and proximate cause, Plaintiffs and Class members have suffered damages as discussed herein, including missed payments and out-of-pocket expenses associated with (i) purchasing new healthcare payment software; (ii) notifying patients of the Data Breach; and (iii) late penalties assessed for untimely payment of expenses. Furthermore, Plaintiffs' and Class members' damages include time and effort spent researching and implementing new healthcare payment software. Plaintiffs and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and have incurred extra costs from switching to another healthcare payment software.

COUNT XIII
Violation of the Washington Consumer Protection Act,
Wash. Rev. Code § 19.86.010, *et seq.*
(On Behalf of Plaintiff Wills and the Nationwide Class, or, Alternatively, the Washington Class)

495. Plaintiff Wills and the Washington Class repeat and reallege every allegation set forth in the preceding paragraphs.

496. Plaintiff Wills, the Washington Class, and Defendants are "person[s]" under Wash. Rev. Code § 19.86.010(1).

497. The Washington Consumer Protection Act (WCPA) prohibits any "unfair or deceptive acts or practices" in the conduct of any trade or commerce. Wash. Rev. Code § 19.86.020.

498. Defendants advertised, offered, or sold services in Washington and engaged in trade or commerce directly or indirectly affecting Plaintiff Wills and Washington Class members under Wash. Rev. Code §§ 19.86.010(2).

499. Defendants engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce under Wash. Rev. Code § 19.86.020, including:

(a) Representing that their goods and services have characteristics, uses, and benefits that they do not have; and

(b) Representing that their goods and services are of a particular standard or quality if they are of another.

500. Defendants' unfair, unconscionable, and deceptive practices include but are not limited to:

(a) Failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols; and software and hardware systems to safeguard and protect their network that powers the Change Platform despite representation otherwise;

(b) Failing to comply with common law and statutory duties pertaining to the security of their network that powers the Change Platform, including duties imposed by Section 5 of the FTCA and HIPAA Privacy and Security Rules;

(c) Failing to properly protect the integrity of the systems powering the Change Platform;

(d) Misrepresenting that Defendants maintained reasonable and adequate security measures;

(e) Misrepresenting that Defendants would comply with common law and statutory duties pertaining to security of their network, including duties imposed by Section 5 of the FTCA and HIPAA Privacy and Security Rules;

(f) Omitting, suppressing, and concealing the material fact that Defendants did not properly secure their systems powering the Change Platform;

(g) Omitting, suppressing, and concealing the material fact that Defendants did not comply with common law and statutory duties pertaining to the security of their network, including duties imposed by Section 5 of the FTCA and HIPAA Privacy and Security Rules; and

(h) Overcharging for services provided without adequate security measures in place.

501. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and the ability to ensure access to the Change Platform.

502. Defendants knowingly and willingly represented that their network maintained adequate protections to induce Plaintiff Wills and the Washington Class to use and rely on Defendants' services.

503. Defendants' concealments, omissions, and false promises inducted Plaintiff Wills and the Washington Class to use and rely on Defendants' services. But for these unlawful acts by Defendants, Plaintiff Wills and the Washington Class would not have used or relied on Defendants' services.

504. The gravity of Defendants' wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendants' legitimate business interests other than engaging in the above-described wrongful conduct.

505. As a direct and proximate result of Defendants' conduct alleged herein and in violation of the WCPA, Plaintiffs and Class members have suffered damages as discussed herein, including missed payments and out-of-pocket expenses associated with (i) purchasing new healthcare payment software/services; (ii) notifying patients of the Data Breach; and (iii) late penalties assessed for untimely payment of expenses. Furthermore, Plaintiffs' and Class members' damages include time and effort spent researching and

implementing new healthcare payment software and services, hiring staff or third-party companies to troubleshoot the business disruption caused by Defendants' shutdown of the Change Platform, obtaining loans or funds—including application fees and interest—to fund operations that they would not have otherwise been obligated to obtain had Defendants timely process and paid their insurance claims. Plaintiffs and Class members have not received payments for their healthcare services or have received late payments depriving them of the time-value of money and loss of interest and have incurred extra costs from switching to another healthcare payment software.

506. Plaintiffs, on behalf of themselves and the Washington Class members, also seek to recover actual damages sustained by each Washington Class member together with the costs of the suit, including reasonable attorney fees.

COUNT XIV
Declaratory Judgment
(On Behalf of Plaintiffs and the Nationwide Class)

507. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

508. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

509. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and other duties to reasonably safeguard

the networks that provide services that Plaintiffs and Class members rely on for claim processing and payment services, and whether Defendants are currently maintaining data security measures adequate to protect patients from further cyberattacks and data breaches that could compromise their PII and PHI and therefore prevent healthcare providers from remaining without use of the Change Platform, which is a lynchpin of their payment practices.

510. Defendants still possess PII and PHI pertaining to patients, which means patients' PII and PHI remains at risk of further breaches because Defendants' data security measures remain inadequate. Another data breach would likely result in Defendants disconnecting the Change Platform again, causing further injuries to Plaintiffs and Class members.

511. Pursuant to the Declaratory Judgment Act, Plaintiffs seek a declaration that: (a) Defendants' existing data security measures do not comply with their obligations and duties of care; and (b) in order to comply with their obligations and duties of care, (1) Defendants must have policies and procedures in place to ensure the parties with whom they share sensitive personal information maintain reasonable, industry-standard security measures, including, but not limited to, those listed at (ii)(a)-(i), *infra*, and must comply with those policies and procedures; (2) Defendants must: (i) purge, delete, or destroy in a reasonably secure manner patients' PII and PHI if it is no longer necessary to perform essential business functions so that they are not subject to further theft; and (ii) implement and maintain reasonable, industry-standard security measures, including, but not limited to:

(a) Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

(b) Engaging third-party security auditors and internal personnel to run automated security monitoring;

(c) Auditing, testing, and training their security personnel regarding any new or modified procedures;

(d) Encrypting PII and PHI and segmenting PII and PHI by, among other things, creating firewalls and access controls so that if one area of Defendants' systems is compromised, hackers cannot gain access to other portions of their systems;

(e) Purging, deleting, and destroying in a reasonable and secure manner PII and PHI not necessary to perform essential business functions;

(f) Conducting regular database scanning and security checks;

(g) Conducting regular employee education regarding best security practices;

(h) Implementing MFA and POLP to combat system-wide cyberattacks; and

(i) Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class set forth herein, respectfully request the following relief:

(a) That the Court certify this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, appoint Plaintiffs as class representatives and Plaintiffs' counsel as Class Counsel;

(b) That the Court grant permanent injunctive relief to prohibit and prevent Defendants from continuing to engage in the unlawful acts, omissions, and practices described herein;

(c) That the Court award Plaintiffs and Class members compensatory, consequential, and general damages, including nominal damages as appropriate, for each count as allowed by law in an amount to be determined at trial;

(d) That the Court award statutory damages, trebled, and/or punitive or exemplary damages, to the extent permitted by law;

(e) That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendants as a result of their unlawful acts, omissions, and practices;

(f) That Plaintiffs be granted the declaratory and injunctive relief sought herein;

(g) That the Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses; and

(h) That the Court award pre-and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a jury trial in the instant action.

Dated: July 19, 2024

/s/E. Michelle Drake
E. Michelle Drake, Bar No. 0387366
BERGER MONTAGUE
1229 Tyler Street NE, Suite 205
Minneapolis, MN 55413
Telephone: (612) 594-5933
emdrake@bm.net

Mark B. DeSanto*
BERGER MONTAGUE
1818 Market Street, Suite 3600
Philadelphia, PA 19103
Telephone: (215) 875-3046
mdesanto@bm.net

Sophia M. Rios*
BERGER MONTAGUE
8241 La Mesa Boulevard, Suite A
La Mesa, CA 91942
Telephone: (619) 489-0300
srios@bm.net

Norman E. Siegel*
J. Austin Moore*
Stefon J. David*
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Telephone: (816) 714-7100
siegel@stuevesiegel.com
moore@stuevesiegel.com
david@stuevesiegel.com

**Pro Hac Vice Forthcoming*

Counsel for Plaintiffs and the Class

JS 44 (Rev. 04/21)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

Agius Psychological Services, LLC, et al.

(b) County of Residence of First Listed Plaintiff Genesee (MI)
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

Berger Montague PC, 1229 Tyler St NE, Ste 205, Minneapolis, MN 55413; 6125945999

DEFENDANTS

Change Healthcare Inc., Optum, Inc., UnitedHealth Group Incorporated

County of Residence of First Listed Defendant
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☒ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☒ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

INTELLECTUAL PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. § 1332(d)(2)

Brief description of cause:
Breach of implied contract, violations of consumer protection statutes, due to data breach

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $

CHECK YES only if demanded in complaint:

JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions):

JUDGE Frank DOCKET NUMBER 0:24-md-03108

DATE 7/19/2024

SIGNATURE OF ATTORNEY OF RECORD /s/E. Michelle Drake

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. Jurisdiction. The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. Residence (citizenship) of Principal Parties. This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. Origin. Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

VI. Cause of Action. Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.

VII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. Related Cases. This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.