Exhibit A1

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CASE NO. 23-61065-CIV-SINGHAL

DONNA CROWE, *et al.*, *on behalf of themselves and all others similarly situated*,

Plaintiffs,

v.

MANAGED CARE OF NORTH AMERICA, INC. d/b/a MCNA DENTAL, MCNA INSURANCE COMPANY d/b/a MCNA DENTAL, and HEALTHPLEX, INC.

Defendants.

AMENDED CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs, Agustin Acosta, Brittney Brown, Montwain Carter, Donna Crowe, Shavonne Diggs, Crystal Gannon, Yvon Hanekom, Samantha Hathaway, Sara Hughes, Tarek Kachakech, Kade McCraw, Heather Shaffer, Aliciah Souza-Shores, Asia Spears, Heidi Winkler, and Franny Zurline ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this Consolidated Class Action Complaint action against Managed Care of North America, Inc. d/b/a MCNA Dental, MCNA Insurance Company d/b/a MCNA Dental ("MCNAIC") (collectively, "MCNA Dental") and Healthplex, Inc. ("Healthplex") (all collectively, "MCNA"). The following allegations are based upon Plaintiffs' personal knowledge as to their own actions and their counsels' investigations, facts of public record, and upon information and belief as to all other matters.

1. This action arises from MCNA's (including, in the case of Plaintiff Tarek Kachakech and the putative New York Subclass, Healthplex) failure to secure the highly sensitive

Joseph J. Tabacco, Jr. (SBN 75484)
Kristin J. Moody (SBN 206326)
Alexander S. Vahdat (SBN 284963)
BERMAN TABACCO
425 California Street, Suite 2300
San Francisco, CA 94104
Telephone: (415) 433-3200
Facsimile: (415) 433-6382
Email: jtabacco@bermantabacco.com
kmoody@bermantabacco.com
avahdat@bermantabacco.com

Local Counsel for Plaintiffs and the Proposed Class

Patricia I. Avery (for admission *pro hac vice*)
Philip M. Black (SBN 308619)
WOLF POPPER LLP
845 Third Avenue
New York, NY 10022
Telephone: (212) 759-4600
Email: pavery@wolfpopper.com
pblack@wolfpopper.com

Attorneys for Plaintiffs and the Proposed Class

SUPERIOR COURT OF THE STATE OF CALIFORNIA
FOR THE COUNTY OF SAN MATEO

ELIZABETH COPLEY and RACHEL CALCATERRA, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

NATERA, INC.

Defendant.

Case No. 23-CIV-03095

AMENDED CLASS ACTION COMPLAINT FOR:

1. **VIOLATIONS OF THE CALIFORNIA UNFAIR COMPETITION LAW (Cal. Bus. & Prof. Code §§ 17200, *et seq.*);**
2. **VIOLATIONS OF THE CALIFORNIA CONSUMER LEGAL REMEDIES ACT (Cal. Civ. Code 1750, §§ *et seq.*);**
3. **BREACH OF IMPLIED CONTRACT OR QUASI-CONTRACT;**
4. **VIOLATIONS OF THE CONNECTICUT UNFAIR TRADE PRACTICES ACT (Conn. Gen. Stat. § 42-110b(a)); and**
5. **VIOLATIONS OF THE FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT (Fla. Stat. § 501.204(1).**

CLASS ACTION

DEMAND FOR JURY TRIAL

Plaintiffs Elizabeth Copley ("Copley") and Rachel Calcaterra ("Calcaterra") (collectively "Plaintiffs"), individually and on behalf of all others similarly situated, bring this action against Natera, Inc. ("Natera" or "Defendant"), and allege on information and belief, except as to the allegations that pertain to Plaintiffs, which are based on their individual, personal knowledge, as follows:

INTRODUCTION

1. Plaintiffs bring this class action on behalf of all persons in the United States who had a "Panorama," "Horizon," "Vistara," or "Spectrum" test performed by Natera, and were then billed more than $249 for that test.

2. Natera is a genetic testing company in San Carlos, California that offers a range of prenatal genetic testing services designed to screen for genetic abnormalities in the prospective parents or the fetus. Through brochures and other communications with patients, usually via patients' medical providers, Natera represents that the out-of-pocket cost to patients for the tests will not exceed $249.

3. However, despite these representations, Natera routinely bills patients several hundred or even thousands of dollars for its tests—much more than the $249 Natera promises. The list price for Natera's tests, which Natera does not reveal to patients in advance, is up to $8,000 per test. Despite Natera's assurance that its tests are affordable and will not cost patients more than $249, Natera instead sends bills for much higher amounts to patients' health insurers and to patients directly, leaving patients on the hook for enormous bills that they did not expect to receive. Natera often bills patients many months or even years after the patient's testing took place, and for amounts well in excess of $249 (e.g., approximately $750, $1600, or even thousands more). Natera will send such bills even if Natera already received more than $249 from a patient's health insurer.

4. Natera's deceptive, unfair, and abusive billing practices cause a substantial financial burden on new, expecting, and prospective parents, at a time when they are already feeling financially vulnerable. Natera's billing practices have been widely panned on websites such as Yelp, Better Business Bureau, Reddit, and What to Expect. For example, as of July 5,

2023, Better Business Bureau has 431 reviews and Yelp has 213 reviews, a majority of which are negative reviews that give the company a "1 star" rating. Similarly, a Reddit thread titled "How is this not fraud? – Natera bill" has 105 comments with people narrating their horror experiences with Natera's billing practices. Over the years, the site whattoexpect.com has also contained several discussion threads titled, e.g., "Natera is a terrible company"; "Beware Natera Billing!"; "Natera Billing issues"; "Natera genetic testing bill $8000?!".

5. When Copley was pregnant with her second child, her OB/GYN recommended a Natera genetic test (the "Panorama" test). She was assured by her OB/GYN's office that the test would not cost more than, at most, $250. However, Copley later received an Explanation of Benefits statement from her insurer showing charges from Natera totaling $8,000 for the test. In response, Copley's husband called Natera, and a Natera representative told him that Copley would be charged $249 for the test, confirming the pricing that Copley had been told at her OB/GYN's office. Nevertheless, over a year and a half later, Copley received a bill from Natera for $721.10, and then received a second and a third bill from Natera for the same amount. After making one payment of $50 to Natera under protest, Copley then received a "final notice" bill dated October 24, 2021 for $671.10, due immediately. As is the case for all other members of the proposed class, the bills Copley received from Natera contradicted Natera's representation that its genetic tests would cost patients no more than $249, and charged grossly in excess of the reasonable value of the services rendered.

6. Plaintiff Calcaterra viewed a Natera brochure at her OB/GYN's office prior to undergoing the Panorama and Horizon tests. That brochure said: "If [Natera] estimate[s] your cost to exceed $249, we'll contact you and you choose how you pay: insurance or cash." It also said: "If we estimate your cost to exceed $249 per test, we'll contact you to discuss cash pay options." An insert inside the brochure further said: "If your insurance does not cover genetic testing, the non-covered service amount is $249." Notwithstanding these representations, Natera later billed Calcaterra demanding payment of $749 for the Horizon test and a further $212.54 for the Panorama test. Calcaterra called Natera and complained that the bills were more than Natera

had represented, but Natera refused to honor the $249 price. Consequently, Calcaterra paid both bills in full.

7. The statement that Natera's tests would cost Plaintiffs not more than $249 originated with Natera in California. Natera's business model relies on having physicians' offices recommend Natera testing to patients. Natera then bills patients separately for the tests, without communicating to patients the true amount that Natera will charge for the tests. Natera decides what it will represent as the charge for its tests, and then communicates that information to patients, as well as to physicians' offices with the knowledge and intent that the information will then be transmitted to patients. As described in more detail below:

- The Natera brochure received by Calcaterra is distributed to patients through their physicians, and explicitly says that patients will have the option of paying a $249 cash price.
- Natera's bills have a section entitled "Who Is Natera?," showing that Natera knows that patients often hear about the company and its tests, including the price thereof, from their physicians, and not from Natera directly.
- Copley's former and current OB/GYNs had relationships with Natera through Natera sales representatives. Both of Plaintiff Copley's OB/GYN's offices were told by Natera representatives that Natera tests would not cost their patients more than, at most, $250.
- When Copley's husband called Natera, the Natera representative confirmed on the phone that Copley would be charged $249 for the test (even though Natera then billed Copley for more than twice this amount).

8. Defendant's conduct with respect to billing for its genetic tests violates the California Unfair Competition Law ("UCL"), the California Consumer Legal Remedies Act ("CLRA"), the Connecticut Unfair Trade Practices Act ("CUTPA"), the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), and common law, which provides that in the absence of an express contract, service providers are entitled to the reasonable value of the services rendered.

PARTIES

9. Plaintiff Elizabeth Copley is a natural person who is a citizen of the United States and who, at all relevant times hereto, has resided and been domiciled in the State of Connecticut.

10. Plaintiff Rachel Calcaterra is a natural person who is a citizen of the United States and who, at all relevant times hereto, has resided and been domiciled in the State of Florida.

11. Defendant Natera, Inc. is incorporated in Delaware and operates one of its two major testing laboratories at 201 Industrial Road, Suite 410, San Carlos, California 94070. Defendant is a corporation that provides prenatal genetic testing services.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction pursuant to California Constitution Article VI, Section 10.

13. This Court has personal jurisdiction over Defendant because Defendant is duly licensed, registered, and conducts business in the State of California, and a substantial portion of the conduct giving rise to Plaintiffs' claims took place in California. The amount in controversy exceeds the jurisdictional minimum of this Court.

14. Venue is proper in this Court because Defendant maintains offices, has agents, employs individuals, and/or transacts business in this jurisdiction; a substantial portion of the conduct giving rise to Plaintiffs' claims occurred in this jurisdiction; and Defendant caused harm to Plaintiffs and putative Class members from within this jurisdiction.

FACTUAL ALLEGATIONS

Background on Natera

15. Natera specializes in providing genetic tests for pregnant women and prospective parents, particularly non-invasive prenatal testing ("NIPT") services. It offers several genetic testing panels with different brand names, including Panorama, Horizon, Vistara, and Spectrum. The Horizon and Panorama panels contribute a significant majority of the company's revenues

(and Natera has publicly stated that it "expect[s] this to continue to be the case"[1]). The company's other tests are currently primarily performed at Natera's San Carlos location.[2]

16. Natera operates laboratories in Austin, Texas and San Carlos, California, both of which process the Panorama and Horizon tests. In the year ended December 31, 2020, Natera processed most of its tests in its San Carlos, California laboratory (*see* Natera's 2020 Form 10-K, retrieved from investor.natera.com, accessed February 22, 2022). Natera's San Carlos laboratory and office space is apparently significantly larger than the laboratory and office space which Natera's subsidiary leases in Austin, and Natera's San Carlos laboratory is currently recognized by 48 U.S. states as a Medicaid provider.

17. Natera's bills are sent from, and are payable to, California addresses, namely PO Box 399023, San Francisco CA 94139-9023, or PO Box 889023, Los Angeles, CA 90088-9023.

18. Natera uses its San Carlos, California address and telephone number on test brochures, including brochures for its most popular tests, Panorama and Horizon.

19. Natera uses its San Carlos, California address on test results.

20. Natera directs patients and providers who have questions to call a phone number with a 650- area code (San Carlos and San Francisco Bay Area) to obtain answers, including within a Natera Billing Guide brochure.

21. Based on the foregoing, Natera's billing policies and practices are established and managed from within California, and Natera receives patient payments in California.

Natera's Deceptive and Unfair Billing Practices

22. Natera's billing policy and practices are deceptive and unfair. Natera sets the prices of its tests and determines the amount to charge insurers and patients for those tests, and also determines what to communicate to patients and providers about the cost of its tests. In so doing, Natera conceals that the list price for its genetic testing services is thousands of dollars,

[1] *See* Natera's 2022 Annual Report to Shareholders, at, *e.g.*, 29.

[2] *Id.* at 37 ("We currently operate laboratory facilities in Austin, Texas and in San Carlos, California, both of which process Panorama, Horizon, and Signatera tests, which together represent the significant majority of our revenues. Our other tests that we perform are currently only able to be performed at one, but not both, of our laboratories, and are primarily performed at our San Carlos location.").

depriving patients of the ability to make an informed decision about whether to undergo those tests. Instead, Natera promises patients, both directly and through marketing channels with medical providers, that the cost to patients will not exceed $249. Natera's billing practices are deceptive and unfair because Natera does not accurately disseminate crucial price information to patients and instead makes false and/or misleading statements about the cost of its tests.

23. Natera fails to ensure that patients are made aware of its billing practices. As a common theme, Natera fails to disclose to patients the extremely high price it charges for its genetic tests (approximately $8,000) and the fact that many insurance plans do not cover these tests, or do not cover portions of them. For example, Natera fails to inform patients that coverage for its tests might be denied as "experimental," and that while some insurance companies may cover the Panorama test, they may nevertheless consider the "microdeletions" add-on to that test as experimental, and deny coverage for that portion of the test (which Natera charges for separately). Since genetic testing remains a fairly new area of medical science and may not be fully covered by some insurance plans, disclosure of the full charge for the tests is especially crucial for patient decision making. Furthermore, where patients have not met their deductible or where their insurance denies coverage, the full $8,000 list price or the amount above what the insurance "allows" (which is often more than $500) becomes the patient's responsibility. Natera does not disclose to patients that Natera will bill them for the amount that their insurance deems the patient responsibility, whether or not it exceeds $249.

24. Natera's website, brochures, and other marketing materials that purport to provide billing and pricing information are misleading and conceal crucial information, the disclosure of which would affect a patient's decision to undergo these tests. Natera recognizes that pricing information is fundamentally important to patients, but nevertheless provides false assurances that patients will not have to pay more than "our cash price" (i.e., $249).

25. For example, a "Natera Billing Guide" brochure states: "If you've met your deductible, the average out-of-pocket expense is less than $249 . . . . If your insurance plan denies the claim, you will be eligible for our discounted cash price." This brochure gives Natera's address in San Carlos, California.

26. Additionally, as of February 22, 2022, on the "Pricing and Billing Information" page under the Women's Health category on Natera's website,[3] Natera stated that it offered "price transparency – rooted in [its] commitment to provide affordable testing for all who can benefit." Natera claimed to provide "clear cost estimates for patients" through a "Price Transparency Program," which includes four steps, namely: (1) "Medical provider orders a test. We start processing the patient sample." (2) "Natera billing issues an insurance estimate." (3) "If we estimate your cost to exceed our cash price, we'll contact you via text or email and you choose how you pay: insurance or cash." (4) "If you choose insurance, Natera billing issues an invoice to you once Natera reviews your health plan's confirmation of exactly how much you owe." As of July 5, 2023 and October 9, 2023, this same webpage contained materially the same information, stating that Natera provides "Personalized Cost Estimates" through its "Price Transparency Program (PTP)," whereby: "If you provide your insurance information, Natera reviews it and if we estimate your out-of-pocket cost to exceed our cash price, we will contact you to discuss alternative payment options." This webpage also states that patients " can receive a personalized cost estimate for Panorama™, Vistara™, Empower™, or Horizon™ by texting us at 1-650-210-7046," a San Francisco Bay area code. However, in practice, Natera neither runs insurance estimates for patients prior to billing nor contacts patients to give them an option to pay through insurance or cash. Instead, Natera surprises patients with huge bills. Natera does not explain to patients that their out-of-pocket cost may exceed $249 if patients choose to utilize their insurance coverage, even if the patient's insurance has already paid that amount (or more) to Natera.

27. Natera's bills will offer some patients a "prompt payment" deal to waive any charges above $249 if the patient pays within a limited time window—a high-pressure tactic that is designed to take advantage of patients and extract as much money as quickly as possible from them. This tactic also admits that the much higher, undisclosed list prices for the tests are unreasonable, have no relationship to the cost to provide the test, and are not what Natera expects to receive from patients. Patients who are not offered the $249 deal, or who do not respond in time, are billed for an unreasonably larger amount.

[3] www.natera.com/womens-health/pricing-billing/

28. Natera induces medical providers to provide misleading billing information to patients by failing to disclose its billing practices to providers, and instead informing them that the cost of its tests to patients will not exceed $249 (or $250). As further alleged below, both Plaintiffs' former and current OB/GYN's offices had relationships with Natera representatives, who told the offices that the cost of Natera testing to patients would not exceed $250. As a result of Natera's marketing to healthcare providers, the providers themselves are given the impression that patients will not owe more than this amount for Natera tests, and convey this information to patients. Natera is aware that this misinformation about the cost of its tests is routinely communicated from providers to patients, and encourages these communications. While providers may pass along a price of $250 instead of $249 to patients, this is merely due to rounding, since the number that appears in Natera's written materials (e.g., billing and brochures) is consistently $249.

29. Natera's bills to patients reflect Natera's awareness that patients may be hearing about Natera for the first time when they receive a bill from Natera. To wit, there is a section on the back of Natera's bills that reads: "Who is Natera? Natera offers non-invasive genetic testing services. Your physician is uncompromising in patient care and asked us to perform important tests on a blood sample collected during your office visit." It further reads: "Why did I receive a Natera Statement? You are receiving a statement/bill from Natera because genetic testing services were performed, on your behalf, at the request of your physician."

30. In addition, Natera will also bill in-network patients exorbitant and improper charges. In these bills, Natera misleadingly claims that the patient's insurance did not cover the test, when, in reality, Natera failed to obtain required pre-authorization(s) from the insurer(s). Consequently, patients who should owe nothing for the test, or only a co-pay, are hit with a surprise bill stating that they owe much more than what they expected. Natera is aware of its obligation to obtain pre-authorization, but intentionally or recklessly does not obtain that pre-authorization. Natera's practice of billing in-network patients is an attempt to circumvent its pre-authorization obligations with insurers by improperly and fraudulently obtaining payment directly from patients.

31. Natera receives an economic benefit from billing patients, even before patients pay those bills. Specifically, Natera's bills generate a receivable asset for Natera.[4] If a patient pays the bill, that receivable asset is converted to cash.

32. Natera's bill represents an economic injury to consumers. Until such time as the bill is retracted, the bill is a liability to the patient (albeit a disputed one), and Natera could take imminent action in furtherance of the enforcement of that asserted liability (through, for example, sending the bill to collections or instituting other legal process).

Experiences with Natera's Billing Policy

Plaintiff Elizabeth Copley

33. For her second pregnancy, Copley received OB/GYN care from a physician's practice in New Milford, Connecticut.

34. Copley's experience illustrates Natera's symbiotic relationship with OB/GYN practices. Copley's practice has maintained a direct relationship with Natera whereby, at some point prior to late 2019, a Natera representative informed the practice that the out-of-pocket cost to patients for any Natera tests not covered by insurance would be $250. As expected, the practice passes this information along to patients on behalf of Natera, including Copley.

35. In late 2019, when Copley was pregnant with her second child, the nurse practitioner at Copley's then-OB/GYN's office advised her to do the Natera Panorama Non-Invasive Prenatal Testing panel ("Panorama panel") due to her age.

36. Upon specifically inquiring how much the test would cost, the nurse practitioner assured Copley that it would not cost more than $250, at most.

[4] *See* https://www.investopedia.com/terms/a/accountsreceivable.asp (accessed June 20, 2023) (explaining that "Accounts receivable (AR) are an asset account on the balance sheet that represents money due to a company in the short term. Accounts receivable are created when a company lets a buyer purchase their goods or services on credit. . . . An example of accounts receivable includes an electric company that bills its clients after the clients received the electricity. The electric company records an account receivable for unpaid invoices as it waits for its customers to pay their bills.")

37. Copley has been told by her former OB/GYN's office that the information on the cost of the Natera test was based on statements and representations made to the OB/GYN's office by Natera's representative.

38. Based on the pricing information that Copley's OB/GYN's office passed along to her from Natera, Copley agreed to get her blood drawn for the "Panorama Prenatal Screen with Microdeletions" panel (procedure codes: Fetal Chromosomal Aneuploidy with Microdeletions 81420HA, 81422HA) on October 22, 2019.

39. Copley did not hear anything further about or from Natera until she noticed a charge of $8,000 on an Explanation of Benefits ("EOB") statement from her insurer, Connecticare, in late 2019 or early 2020. The EOB was for the plan year 01/01/2019 to 12/31/2019. Natera had billed Connecticare $3,900 for Pathology services and $4,100 for Laboratory services in connection with the Panorama panel. Connecticare denied the claim entirely, transferring potentially the entire charge onto Copley.

40. After receiving the EOB, Copley's husband, Charles Copley, called Connecticare inquiring about the charge. Connecticare advised him to call Natera.

41. Charles Copley then called Natera inquiring about the charge. He informed the Natera representative to whom he spoke that he and his wife were completely unaware that they could be charged thousands of dollars for the Panorama panel, a situation vastly different from what Copley's OB/GYN's office had earlier represented to Copley about the cost of the test.

42. The Natera representative responded by saying that Copley would be charged $249 for the test, thereby confirming the pricing that Copley had been told by her OB/GYN's office. The Natera representative never advised Copley or Copley's husband that her doctor's office was mistaken, had misspoken, or had otherwise given any incorrect information to Copley about Natera's prices.

43. However, over a year and a half later, Natera sent Copley a bill dated July 9, 2021 for $721.10 for the very same test, more than double the amount communicated to Copley at her OB/GYN's office and later confirmed by Natera's representative. The bill was due on August 8, 2021.

44. After receiving the bill from Natera, Charles Copley called Natera again, and expressed that he thought he had already paid the bill.

45. However, Natera sent Copley a second bill dated August 16, 2021 for $721.10, due upon receipt.

46. Natera then sent Copley a third bill dated September 17, 2021 for $721.10, due upon receipt. This bill stated that the bill was "past due," and further stated: "To prevent your account from going to a professional collections agency, please submit payment for the amount due immediately."

47. In response to these bills, Copley made one payment of $50 to Natera by check, noting on the check that it was paid under protest.

48. Copley later received a bill dated October 24, 2021 for $671.10, due immediately. This bill stated that it was a "final notice," and further stated: "To prevent your account from going to a professional collections agency, please submit payment for the amount due immediately." While Copley disputes that she owes this amount to Natera, it is her understanding that Natera expects that she will pay this bill, and that it could be sent to collections at any time. Natera has not retracted this bill.

49. All of the bills that Natera sent to Copley were sent from, and payable to, Natera at PO Box 399023, San Francisco CA 94139-9023.

50. Based on Natera's conduct, i.e., the fact that Natera had a relationship with Plaintiff's former OB/GYN's office and sent Copley a bill, it is evident that Natera believed it was authorized to send Copley a bill and also believed that Copley was obligated to pay it.

51. Had Copley been aware of the true price of the Panorama test and the amount she would be charged by Natera, she would not have agreed to do the test at that time, and thus would not have paid Natera any money at all.

52. Since Plaintiff's prior experience with Natera, Copley has become pregnant again and again underwent Natera testing recommended by her current OB/GYN. At her current OB/GYN's office, prior to undergoing the test on or about May 28, 2023, she received an information sheet stating that "maximum" cost for the Panorama test would be $249.

Nevertheless, on or about May 30, 2023, Copley received an email from Natera stating that her "estimated out-of-pocket cost" would actually be $720-820.

53. Plaintiff's current OB/GYN's office also deals directly with Natera, and has likewise been told by Natera that the out-of-pocket cost to patients for Natera tests would not exceed $249, confirming that this misrepresentation comes from Natera.

Plaintiff Rachel Calcaterra

54. In February 2022, Calcaterra was recommended Natera testing by her OB/GYN, located in Fort Myers, Florida.

55. Prior to having her blood drawn, a midwife at Calcaterra's OB/GYN's office handed Calcaterra a Natera brochure.

56. The brochure stated: "If [Natera] estimate[s] your cost to exceed $249, we'll contact you and you choose how you pay: insurance or cash." It also said: "If we estimate your cost to exceed $249 per test, we'll contact you to discuss cash pay options." An insert inside the brochure further said: "If your insurance does not cover genetic testing, the non-covered service amount is $249."

57. Both the brochure and the insert provided the contact information for Thomas O'Brien, identified in the brochure as an account sales representative for Natera. The brochure listed Natera's San Carlos, California address under Mr. O'Brien's name, but gave his phone number beginning with a 239- (Fort Meyers, Florida) area code.

58. Based on the content of the brochure and insert, Calcaterra's OB/GYN's office maintained a direct relationship with Natera.

59. The brochure listed Natera's address as 201 Industrial Road, Suite 410, San Carlos, CA 94070, and phone number as +1 650.249.9090.

60. Based on the pricing information in the Natera brochure, Calcaterra decided to undergo the Panorama and Horizon tests, and had her blood drawn for those tests on or about February 22, 2022.

61. Without contacting Calcaterra, Natera apparently submitted claims for the tests to her insurer, which did not pay the entire cost of the tests.

62. Natera then billed Calcaterra $10,505 for the Horizon test, which was adjusted down to an amount due of $749, in an invoice dated March 23, 2022. Natera sent another invoice for this amount dated April 19, 2022.

63. Natera also billed Calcaterra $8,000 for the Panorama test, which was adjusted down to an amount due of $212.54, in an invoice dated July 28, 2022.

64. Both sets of bills were payable to Natera at PO Box 889023, Los Angeles, CA 90088-9023.

65. Calcaterra called Natera to inform Natera that she thought the out-of-pocket price should be $249 for the Horizon test based on the written materials she had seen; however, the Natera representative to whom she spoke would not honor that price.

66. Consequently, Calcaterra paid the entire balance of both bills, including $749 for the Horizon test.

67. Had Calcaterra been aware of the true price of the Horizon test and the amount she would be charged by Natera, she would not have agreed to do the test at that time, and thus would not have paid Natera any money at all.

Other experiences

68. Just like Plaintiffs, hundreds, if not thousands, of other people have had similar experiences with Natera's deceptive and unfair billing practices, and many have left reviews on websites including Yelp, Better Business Bureau ("BBB"), Reddit, and What to Expect. These reviews mention Natera's conduct in concealing the price of Natera genetic tests; surprise balance billing patients after recovering a portion from third-party payors (i.e. insurance companies); misleading patients about their out-of-pocket costs for a Natera genetic test; making false statements regarding Natera's purported Price Transparency Program; and harassing patients by repeatedly sending bills even after they have paid Natera's "prompt pay" discount in exchange for the rest of charges being waived.

69. Online reviews on Yelp (yelp.com/biz/natera-san-carlos, accessed on February 8, 2022 and September 14, 2022 and July 5, 2023) confirm that Natera's billing practices are consistent, longstanding, and affecting patients throughout the country.

a. One Yelp reviewer, in a review dated June 26, 2020, wrote: "Terrible company who preys on vulnerable families. We received a bill for $1,590 despite our OBGYN saying the cost is $249 if insurance does not cover it. When we called customer support they confirmed that the rate was $249 but because we didn't respond within 30 days the pricing went up to $1,590. How is that even possible? Stay as far away as you can."

b. Another Yelp reviewer, in a review dated July 7, 2021, wrote: "[W]hat Natera is doing takes the cake. They advertise this 'Price Transparency Program' and tell ordering providers that at most the test will cost us $249 if insurance doesn't pay. What they advertise is, someone checks the coverage/benefits, makes an estimate, and contacts the patient if it might be in their interest to pay self-pay at $249. What they ACTUALLY do is, per the authorization to file insurance you sign on the order, file your insurance and if your insurance pays they take that money and if your insurance leaves you more than $249 out-of-pocket you get a one-time offer for a prompt pay discount of $249, then they go back to trying to bill you the massive coinsurance. In our case insurance paid them over $2k and left us about $1800. They used that $1800 and the fact that my wife authorized insurance to be filed (in the event that it would be better for us than $249) to extort us for the additional $249."

c. In a Yelp review dated January 13, 2022, a reviewer remarked: "Super funny how on the forms you fill out before sending in the sample says 'if your insurance doesn't cover the cost, your maximum payment will be $249', the. [sic] You get a bill in the mail that says you owe over $2700, but your insurance paid over $600 already. When I called and asked what happened the lady on the line goes, we can offer you the $249 deal, but you have to pay with a credit card now.[] Not sure why I still have to pay

$249 when they already stole over $600 from BCBS. Very strange, I'd like some answers from them, but no one speaks English on the hotline."

d. Another Yelp reviewer wrote on December 22, 2022: "I have reported Natera to CMS for their deceptive billing practices after having received a surprise NIPT testing bill for $749 despite their website claiming that the out-of-pocket cost for the bloodwork was around $249 at the time. They billed my in-network insurance an egregious $3,900 for the bloodwork when I clicked the button 'Send to Insurance' instead of clicking the button to pay now. When you call the company, they claim that the initial $249 price was a 'promotional' price that has since expired."

70. On Natera's Better Business Bureau ("BBB") profile (https://www.bbb.org/us/ca/san-carlos/profile/laboratory-research/natera-1116-537368/complaints, accessed on Oct. 27, 2021 and September 14, 2022 and July 5, 2023; and https://www.bbb.org/us/tx/austin/profile/laboratory-testing/natera-inc-0825-1000218084/complaints, accessed on October 9, 2023), patients' reported experiences are no different.

a. One BBB reviewer wrote: "We were told by our fertility clinic for genetic testing out of pocket cost would be $200 each test which we had 2 done mine and my spouse. We were given a paper with this information and told the genetic testing company would contact us once talking to our insurance and [if] it was more than $200 we could do the self-pay option. Nobody ever contacted us and they billed each of our insurance over $14,000 and now insurance is stating we owe an upward of $7000. Nobody ever contacted us to tell us this and offer us the self-pay option……"

b. Another BBB reviewer wrote on August 14, 2022: "Was told the test would only cost $250 and that my insurance covers the cost 100%. 6 months later the charge is finally charged to my insurance for $3900. This charge was also denied through my insurance. Natera mislead me in the

cost and coverage of this testing. I was baited and taken advantage of to get me to agree to this test and now in stuck with a large [bill] I cannot afford to pay."

c. Another BBB reviewer wrote on June 27, 2023: "Assuming the bill that we received is legitimate (which I'm not sure it is) they waited `1.5 years to send us a bill that they said would be $249 if we paid it within 30 days of the invoice date, but $1,590 if we paid after that. We left the country before the bill arrived, a bit more than two weeks after the 'invoice date.' So, by the time we got back into the country and got our mail, we had already passed the 30 days. I am wondering if this is a scam because I can't imagine a legitimate company would do something like this."

d. Another BBB reviewer wrote on September 15, 2023: On April 12, 2023, I went . . . for an ob/gyn visit for my pregnancy. The doctor and nurse suggested I do a genetic screening though Natera because of my advanced maternal age. They gave me several pamphlets from Natera that state that "If we estimate your cost to exceed $249, we'll contact you and you choose how you pay: insurance or cash." The nurse also said that people who pay for the tests and don't have insurance never pay more than $249. . . . I didn't hear anything from Natera for several weeks. I finally looked at my insurance claims online and was shocked to see that Natera had billed Anthem BCBS $4,899.00 and Anthem had flagged most of it as out-of-network. Natera then sent me a bill for $749.00 . . . saying they had adjusted the amount down. I called them concerning this issue and emailed them but received no explanation for their lies or a possible resolution. They lied in the pamphlets saying they would contact me if it cost more than $249. They lied on their website and in the pamphlets saying they are in-network with my insurance. This fraudulent dishonesty is unacceptable.

I want them to adjust my bill to $249 which is still double what other companies charge for similar tests."

e. Another BBB reviewer wrote on September 20, 2023: "On 5/31/2023 I took a Natera Horizons test. My doctor told me it would [cost] $249 out-of-pocket, but that I should go through insurance because it might be less. She told me numerous times that under no circumstances would I be charged more than $249. In August I got an Explanation of Benefits from my insurance company saying that my anticipated cost was $1399.10. When I called Natera, they refused to guarantee that I would not be charged more than $249, but I should wait for my bill to come and call back. When I told the doctor's . . . about this, they said that they have an agreement with Natera and again told me that I would not have to pay more than $249. I got the bill today (9/19/2023) and it was for $749. . . . It also seems like a predatory business practice to tell people they can pay $249 if they pay out of pocket, and then charge three times as much if they go through insurance. Not everyone has the time to make these phone calls and be on top of all these medical bills."

71. The Capitol Forum, an investigative news organization located in Washington, D.C., published an article on August 5, 2021, entitled "Natera: Experts Raise Concerns About Size of Prompt Pay Discounts and Company Billing Practices." This article discusses the experience of multiple patients who were billed hundreds or thousands of dollars more than Natera's advertised cash price of $249 for its tests. The article noted that "Natera patients interviewed by The Capitol Forum shared similar stories regarding Natera's price transparency program and prompt payment discounts. All said that the amounts Natera charged both their insurers and them were far above what they had initially been told by the company, and that Natera sent almost daily emails reminding them to pay." The article also referred to a "fertility clinic in California," which had a "business relationship with Natera," and reported that the clinic "'received a lot of complaints from patients regarding Natera's billing practices'" because Natera

would improperly "'send a bill ranging from $600 to $1000 to both [the clinic] and the patient more than 50% of the time. . . . They harass the patient and they tell them the clinic hasn't paid and you need to pay the bill, calling and emailing them every day, even when [the clinic] already paid the bill sent to [the clinic].'"

72. Patients generally encounter Natera's misrepresentations only before or during pregnancy. Due to the time it takes to carry a pregnancy to term, and the inherent contingencies involved in family planning, patients who have been harmed by Natera's misrepresentations cannot be sure if, or exactly when, they will encounter Natera's misrepresentations again. This is because patients may not choose to become pregnant again, but if they do, there is no guarantee of success, nor can it be predicted when a patient may become pregnant again, or attempt to become pregnant again. However, Natera's billing policies and practices will affect any patient who does become pregnant, or attempt to become pregnant, and undergo genetic testing through Natera.

73. As described herein, Natera knows that the price of its tests is a material piece of information to patients, and intentionally deprives patients of this information. Instead, Natera directly or indirectly falsely promises them a lower price, with the intention of inducing them to undergo its tests with the expectation of an affordable price, only to bill them for an egregiously higher amount at a time when they are already under considerable stress, to patients' financial harm and Natera's benefit.

74. Given the circumstances described hereinabove, Defendant's misconduct is malicious, oppressive, and/or fraudulent.

75. Defendant's conduct constitutes malice because it is intended by the Defendant to cause injury to the Plaintiffs and/or is despicable conduct which is carried on by the Defendant with a willful and conscious disregard of the rights or safety of others.

76. Defendant's conduct constitutes oppression because it is despicable conduct that subjects a person to cruel and unjust hardship in conscious disregard of that person's rights.

77. Defendant's conduct constitutes fraud because Defendant is committing an intentional misrepresentation, deceit, or concealment of a material fact known to the Defendant

with the intention on the part of the Defendant of thereby depriving a person of property or legal rights or otherwise causing injury.

78. Natera's deceptive billing practices, as alleged herein, continue through the present day.

Prior Litigation

79. On November 18, 2021, Copley filed a lawsuit against Natera in the United States District Court for the Northern District of California (case no. 3:21-cv-08941), alleging substantially the same conduct as alleged herein. On May 8, 2023, that federal court dismissed the complaint for lack of standing under Article III of the U.S. Constitution. The decision expressly did not address the merits of Plaintiff Copley's claims or Plaintiff Copley's statutory standing, and was "without prejudice to being filed in state court." ECF No. 64 at 1, 12.

CLASS ACTION ALLEGATIONS

80. Pursuant to California Code of Civil Procedure § 382, Plaintiffs bring this action on behalf of a class of all persons in the United States who had a "Panorama," "Horizon," "Vistara," or "Spectrum" test performed by Natera, and were then billed more than $249 for that test (the "Class"). Copley also brings this action pursuant to California Code of Civil Procedure § 382, on behalf of a subclass of all persons in the State of Connecticut who had a "Panorama," "Horizon," "Vistara," or "Spectrum" test performed by Natera, and were then billed more than $249 for that test (the "Connecticut Subclass"). Calcaterra also brings this action pursuant to California Code of Civil Procedure § 382 behalf of a subclass of all persons in the State of Florida who had a "Panorama," "Horizon," "Vistara," or "Spectrum" test performed by Natera, and were then billed more than $249 for that test (the "Florida Subclass").[5]

81. Upon completion of discovery with respect to scope of the Class, Plaintiffs reserve the right to amend the Class definitions. Excluded from the Class are Defendant, its parents, subsidiaries and affiliates, directors and officers, and members of their immediate families.

[5] Unless specifically indicated otherwise, all allegations below concerning the Class include and apply equally to the Subclasses.

82. This action has been brought and may properly be maintained as a class action because there is a well-defined community of interest in the litigation, the proposed Class and Subclasses are ascertainable because the class definition uses objective terms that make the eventual identification of class members possible, and Plaintiffs are proper representatives of the putative Class and respective Subclasses.

83. The members of the Class and Subclasses are so numerous that the joinder is impracticable. It is believed that at a minimum, thousands of persons across the United States, including in each of Connecticut and Florida, where the respective Plaintiffs reside and are domiciled, have received bills in excess of $249 from Natera for these genetic tests, and thousands more will continue to be subjected to these exorbitant bills if Defendant's practices are not stopped. The precise number of Class and Subclass members and their identities are unknown to Plaintiffs at this time but may be determined through discovery. These members may be notified of the pendency of this action by mail, email, and/or publication through the distribution records of Defendant (and, to the extent applicable, third-party retailers and vendors).

84. Plaintiffs' respective claims are typical of the claims of the Class and Subclass because they had a "Panorama," "Horizon," "Vistara," or "Spectrum" test performed by Natera, and were then billed more than $249 for that test.

85. Plaintiffs will fairly and adequately represent and protect the interests of the other Class and Subclass members. Plaintiffs have no interests antagonistic to those of other Class and Subclass members. Plaintiffs are committed to the vigorous prosecution of this action and have retained counsel experienced in litigation of this nature.

86. Common questions of law and fact exist as to all members of the Class and Subclasses and predominate over any questions affecting only individual members, including, but not limited to:

a. whether Defendant misrepresents its billing and pricing policy to patients, either directly or through patients' medical providers, through its brochures and other channels of marketing;

b. whether Defendant conceals the extremely high price it charges for its genetic panels, thereby deceiving class members into choosing to perform the genetic panels;

c. whether Defendant's conduct constituted an unfair, unlawful, and/or fraudulent business practice in violation of the Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, et seq.;

d. whether Defendant's conduct violated the Consumer Legal Remedies Act, Cal. Civ. Code §§ 1750, et seq.;

e. as to the Connecticut Subclass, whether Defendant's conduct violated the Connecticut Unfair Trade Practices Act, Conn. Gen. Stat. § 42-110a et seq.;

f. as to the Florida Subclass, whether Defendant's conduct violated the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. § 501.204(1);

g. whether Defendant was unjustly enriched as a result of Defendant's conduct;

h. whether Defendant's conduct damaged members of the Class and Subclasses and, if so, the measure of those damages;

i. whether Plaintiffs and the Class are entitled to punitive damages; and

j. whether Defendant's practices in connection with billing of its genetic panels should be enjoined.

87. A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Since the damages suffered by individual Class and Subclass members may be relatively small, the expense and burden of individual litigation make it virtually impossible for the respective Class and Subclass members to seek redress for the wrongful conduct alleged. Plaintiffs know of no difficulty which will be encountered in the management of this litigation that would preclude its maintenance as a class action.

88. Class certification is also appropriate because the Defendant has acted on grounds that apply generally to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the Class as a whole.

89. Class members have suffered and will suffer irreparable harm and damages as a result of Defendant's wrongful conduct.

CAUSES OF ACTION

FIRST CAUSE OF ACTION
Violations of the California Unfair Competition Law
Cal. Bus. & Prof. Code §§ 17200, et seq.
On Behalf of the Class

90. Plaintiffs hereby incorporate by reference all allegations made in the previous paragraphs.

91. Plaintiffs brings this claim individually and on behalf of the members of the Class against Defendant.

92. Plaintiffs assert this cause of action against Defendant for unlawful, unfair and fraudulent business practices; and unfair, deceptive, untrue and misleading advertising, as defined by California's Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, et seq. (the "UCL").

93. Defendant's conduct violates the UCL, as the acts and practices of Defendant constitute a common and continuing course of conduct by means of "unlawful" "unfair" and "fraudulent" business acts or practices within the meaning of the UCL.

94. Defendant's conduct is fraudulent, and thus amounts to unfair competition as set forth in the UCL, in that Defendant conceals the price of its genetic tests and misrepresents the price patients would potentially have to pay for its genetic tests. Such misrepresentations and omissions are likely to deceive, and in fact have deceived, thousands of patients.

95. Defendant's conduct is unlawful, and thus amounts to unfair competition as set forth in the UCL, in that it violates, among other things, California Civil Code §§ 1572, 1709 and 1710, as well as California Business & Professions Code § 17500. As described above, Defendant willfully deceived Plaintiffs and Class members by misrepresenting the price patients would potentially have to pay for its genetic tests, concealing the amount it charges for its genetic tests,

and misrepresenting its billing practice with the intent to induce them to alter their positions to their injury. Defendant's representations were untrue and misleading and Defendant knew, or by exercising reasonable care should have known, such representations were untrue and misleading. Defendant disseminated these untrue and misleading representations as part of a plan or scheme with the intent not to sell its services as so marketed. Defendant knowingly received and retained wrongful benefits and funds from Plaintiffs and members of the Class. Therefore, the Defendant acted with conscious disregard for the rights of Plaintiffs and members of the Class.

96. Defendant's conduct is unfair, and thus amounts to unfair competition as set forth in the UCL, because its utility to Defendant, if any, is greatly outweighed by the harm it causes to Plaintiffs and members of the Class, and because it is immoral, unethical, oppressive, unscrupulous and substantially injurious to patients who end up with unexpected huge bills that cause severe financial distress.

97. As a direct and proximate cause of Defendant's violations of the UCL, Plaintiffs and members of the Class suffered an injury in fact and have suffered monetary harm. Defendant, on the other hand, has been unjustly enriched and should be required to make restitution to Plaintiffs and the Class and/or disgorge its ill-gotten profits pursuant to Business & Professions Code § 17203.

98. Defendant's unlawful, unfair, and fraudulent business practices, as described herein, present a continuing threat to Plaintiffs, the Class and the general public in that Defendant continues to misrepresent the price and out-of-pocket expenses that patients would have to bear for its genetic tests.

99. A constructive trust should be imposed upon all wrongful or inequitable proceeds received by Defendant traceable to Plaintiffs and members of the Class.

100. Plaintiffs and the Class seek equitable relief because they have no other adequate remedy at law. Absent equitable relief, Defendant will continue to injure consumers, and harm the public's interest, thus engendering a multiplicity of judicial proceedings.

101. Plaintiffs further seek an order enjoining Defendant from engaging in any unlawful or inequitable acts and practices as alleged herein, because of Defendant's continuing misrepresentations and improper billing practices.

SECOND CAUSE OF ACTION
Violations of the California Consumer Legal Remedies Act
Cal. Civ. Code §§ 1750, et seq.
On Behalf of the Class

102. Plaintiffs hereby incorporate by reference all allegations made in the previous paragraphs.

103. Plaintiffs brings this claim individually and on behalf of the members of the Class against Defendant.

104. The conduct of Defendant alleged above constitutes an unfair method of competition and unfair or deceptive act or practice in violation of the Consumers Legal Remedies Act, Cal. Civ. Code § 1750, et seq. ("CLRA").

105. Defendant is a person as defined by Cal. Civ. Code § 1761(c).

106. Plaintiffs and Class members are consumers as defined by Cal. Civ. Code § 1761(d).

107. Defendant's genetic testing services described above constitutes a service as defined by Cal. Civ. Code § 1761(b).

108. Plaintiffs' purchases were a transaction under Cal. Civ. Code § 1761(e).

109. The CLRA prohibits "unfair or deceptive acts or practices undertaken by any person in a transaction intended to result or that results in the sale . . . of services to any consumer," which, among other instances enumerated in the CLRA, include: "Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have …." (§ 1770(a)(5)); "Advertising goods or services with intent not to sell them as advertised" (§ 1770(a)(9)); or "a transaction confers or involves rights, remedies, or obligations which it does not have or involve, or which are prohibited by law" (§ 1770(a)(14)).

110. Defendant violated Cal. Civ. Code § 1770(a)(5) by misrepresenting that its genetic testing services have the characteristics of price transparency and a maximum out-of-pocket cost of $249, which in fact they do not.

111. Defendant violated Cal. Civ. Code § 1770(a)(9) by falsely advertising its genetic testing services to be affordable and price transparent; and falsely advertising that it would offer patients the option of paying a discounted cash discount price of $249; and falsely advertising a maximum out-of-pocket cost of $249.

112. Defendant violated Cal. Civ. Code § 1770(a)(13), by making false or misleading statements of fact concerning reasons for, existence of, or amounts of, price reductions of its tests to $249.

113. Defendant violated Cal. Civ. Code § 1770(a)(14) by representing that its transactions with patients involve rights and obligations regarding price transparency and a maximum out-of-pocket cost of $249 which, in fact, they do not have or involve.

114. Defendant violated Cal. Civ. Code § 1770(a)(16) by representing that its tests have been supplied in accordance with a previous representation about price transparency and a maximum out-of-pocket cost of $249, when they have not.

115. The representations and omissions set forth above are of material facts that a reasonable person would have considered important in deciding whether or not to purchase Defendant's services. Plaintiffs and Class members justifiably acted or relied upon Defendant's misrepresentations and omissions to their detriment.

116. Plaintiffs and the other members of the Class have been, and continue to be, injured as a direct and proximate result of Defendant's violations of the CLRA.

117. Plaintiffs are entitled to pursue a claim against Defendant on behalf of the Class to enjoin Defendant from continuing its unfair or deceptive acts or practices under Cal. Civ. Code § 1780(a) and § 1781, as well as to pursue costs and attorneys' fees under § 1780(e).

118. On November 19, 2021, Copley served Defendant with written notice of its CLRA violations pursuant to Cal. Civ. Code § 1782, via letter sent by certified mail, return receipt requested. After the requisite thirty days, Defendant failed to respond to this CLRA notice letter,

and did not make any appropriate correction, repair, replacement, or other remedy. On September 8, 2023, Copley and Calcaterra served Defendant with further written notice of its CLRA violations pursuant to Cal. Civ. Code § 1782, via letter sent by certified mail, return receipt requested. After the requisite thirty days, Defendant failed to respond to this CLRA notice letter, and did not make any appropriate correction, repair, replacement, or other remedy. Pursuant to Cal. Civ. Code § 1782, Plaintiffs are thus entitled to seek damages at this time. Accordingly, Plaintiffs seeks damages on behalf of themselves and the Class as permitted by Cal. Civ. Code § 1782.

THIRD CAUSE OF ACTION
Breach of Implied Contract or Quasi-Contract On Behalf of the Class

119. Plaintiffs hereby incorporate by reference all allegations made in the previous paragraphs.

120. Plaintiffs brings this claim individually and on behalf of the members of the Class against Defendant.

121. A contract is implied by law between the Defendant and the Plaintiffs and Class members, entitling Plaintiffs and Class members an accurate representation of the charges for Defendant's services.

122. A contract is also implied by law between the Defendant and the Plaintiffs and Class members, entitling Defendant to fair market or reasonable value of the testing services rendered (the quantum meruit of the services performed).

123. Defendant breached the terms of the implied contract by billing Plaintiffs and Class members at excessive rates, much higher than reasonable value implied in law, which Plaintiffs and Class members were completely unaware of.

124. By means of Defendant's wrongful conduct alleged herein, Defendant knowingly misrepresented the charges for its genetic tests in a manner that was unfair, unconscionable and oppressive, and knowing the charges would have had an influence in the consumers' decision to purchase the service.

125. As a result of Defendant's wrongful conduct as alleged herein, Defendant has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and members of the Class.

126. Under the common law doctrine of unjust enrichment, it is inequitable for Defendant to be permitted to retain the benefits it received, and is still receiving, without justification, from the imposition of charges upon members of the Class in an unfair, unconscionable, and oppressive manner. Defendant's retention of such funds, under circumstances making it inequitable to do so, constitutes unjust enrichment.

127. Defendant knowingly received and retained wrongful benefits and funds from Plaintiffs and members of the Class. Therefore, the Defendant acted with conscious disregard for the rights of Plaintiffs and members of the Class.

128. Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein.

129. The financial benefits derived by Defendant rightfully belong to Plaintiffs and members of the Class. Defendant should be compelled to provide restitution, and to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and the Class, all proceeds received from Plaintiffs and the Class as a result of any unlawful or inequitable act described herein that unjustly enriched Defendant.

130. A constructive trust should be imposed upon all wrongful or inequitable proceeds received by Defendant traceable to Plaintiffs and members of the Class.

131. Plaintiffs further seek an order enjoining Defendant from engaging in any unlawful or inequitable acts and practices as alleged herein, because of Defendant's continuing misrepresentations and improper billing practices.

132. Plaintiffs and members of the Class have no adequate remedy at law.

FOURTH CAUSE OF ACTION
Violations of the Connecticut Unfair Trade Practices Act
Conn. Gen. Stat. § 42-110b(a)
On Behalf of the Connecticut Subclass

133. Copley hereby incorporates by reference all allegations made in the previous paragraphs.

134. Copley brings this claim individually and on behalf of the members of the Connecticut Subclass against Defendant.

135. The Connecticut Unfair Trade Practices Act ("CUTPA") prohibits "unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce." Conn. Gen. Stat. § 42-110b(a).

136. Defendant's conduct violates the CUTPA because it (1) offends public policy as it has been established by statutes, the common law, or otherwise; (2) is immoral, unethical, oppressive, or unscrupulous; and (3) causes substantial injury to consumers.

137. Defendant further violated the CUTPA by failing to make advertised items conspicuously and readily available for sale at or below the advertised prices. Regs., Conn. State Agencies § 42-110b-18(i).

138. Copley, on behalf of herself and the Connecticut Subclass, seeks damages, punitive damages, injunctive relief, other equitable relief, costs, and attorneys' fees as permitted by Conn. Gen. Stat. § 42-110g.

FIFTH CAUSE OF ACTION
Violations of the Florida Deceptive and Unfair Trade Practices Act
Fla. Stat. § 501.204(1)
On Behalf of the Florida Subclass

139. Calcaterra hereby incorporates by reference all allegations made in the previous paragraphs.

140. Calcaterra brings this claim individually and on behalf of the members of the Florida Subclass against Defendant.

141. The Florida Deceptive and Unfair Trade Practices Act ("FDUTPA") prohibits "[u]nfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce." Fla. Stat. § 501.204(1).

142. Defendant violated the FDUTPA because Defendant's conduct as alleged herein was likely to deceive a consumer acting reasonably in the same circumstances, and that conduct caused actual damages to Calcaterra and members of the Florida Subclass.

143. Calcaterra, on behalf of herself and the Florida Subclass, seeks damages, injunctive relief, other equitable relief, costs, and attorneys' fees as permitted by Fla. Stat. § 501.211 and § 501.2105.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, request that the Court award the following relief:

a. Certify this action as a class action pursuant to California Code of Civil Procedure § 382, appoint Plaintiffs as representative of the Class and their respective Subclasses, and designate the undersigned as Class Counsel;

b. Declare Defendant's conduct unlawful and enter an order enjoining the Defendant from continuing to engage in the conduct alleged herein;

c. Award Plaintiffs and the Class damages, including punitive damages pursuant to Cal. Civ. Code 3294 (and/or to the Connecticut Subclass pursuant to Conn. Gen. Stat. § 42-110g);

d. Award Plaintiffs and the Class restitution and/or disgorgement to the extent legal remedies are unavailable or insufficient;

e. Award pre-judgment and post-judgment interest;

f. Grant Plaintiffs and the Class payment of the costs of prosecuting this action, including expert fees and expenses;

g. Grant Plaintiffs and the Class payment of reasonable attorneys' fees; and

h. Grant such other relief as the Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs and the Class members demand a trial by jury on all triable issues.

///

///

///

DATED: November 8, 2023

Respectfully submitted,

BERMAN TABACCO

By: */s/ Alexander S. Vahdat*
Alexander S. Vahdat

Joseph J. Tabacco, Jr.
Kristin J. Moody
425 California Street, Suite 2300
San Francisco, CA 94104
Telephone: (415) 433-3200
Facsimile: (415) 433-6382
Email: jtabacco@bermantabacco.com
kmoody@bermantabacco.com
avahdat@bermantabacco.com

Attorneys for Plaintiffs and the Proposed Class

Patricia Avery (admission *pro hac vice to be filed*)
Philip M. Black (SBN 308619)
WOLF POPPER LLP
845 Third Avenue
New York, NY 10022
Telephone: (212) 759-4600
Facsimile: (212) 486-2093
Email: pavery@wolfpopper.com

Attorneys for Plaintiffs and the Proposed Class

personal identifiable information ("PII") and protected health information ("PHI") (collectively "Private Information") of Plaintiffs and the members of the proposed Class and State Subclasses (defined *infra* ¶¶ 198, 200) for whom MCNA performed services.

2. MCNA is one of the largest government-sponsored dental insurance providers in the United States, serving over 5 million children and adults through Medicaid, Children's Health Insurance Program ("CHIP"), and Medicare.[1] Therefore, MCNA's customer base is comprised of some of the most financially sensitive individuals, who are either on a fixed income as retirees or lack a financial safety net to afford the impacts of MCNA's failure to secure their sensitive personal information. In this role, for years, MCNA directly and indirectly collected Private Information from millions of customers. Despite having duties created by statute and common law to safeguard that Private Information entrusted to it, MCNA allowed information concerning millions of people to be stolen and posted on the Internet by a notorious cybercriminal organization.

3. On or about February 26, 2023, hackers first gained access to MCNA's network and stole data containing patients' full name, address, date of birth, telephone number, email address, Social Security number, driver's license number, government-issued ID number, health insurance information (including plan information, insurance company, and member number), Medicaid-Medicare ID number, information about medical care or treatment (visits, dentist name, doctor name, past care, x-rays/photos, medicines, and treatment), and bills and insurance claims (the "Data Breach").[2]

4. MCNA's investigation concluded that the Private Information compromised in the

[1] https://www.mcna.net/en/company-overview (last visited Nov. 11, 2023).
[2] Bill Toulas, *MCNA Dental data breach impacts 8.9 million people after ransomware attack*, May 29, 2023, https://www.bleepingcomputer.com/news/security/mcna-dental-data-breach-impacts-89-million-people-after-ransomware-attack/ (last visited Nov. 11, 2023).

Data Breach included the information of Plaintiffs and approximately 8,923,662 other individuals, including patients, parents, guardians, or guarantors (collectively, "Customers").[3]

5. On March 7, 2023, the LockBit ransomware operation claimed responsibility for the Data Breach.[4] LockBit demanded $10 million or threatened to publish 700 GB of sensitive, confidential information they allegedly exfiltrated from MCNA's computer networks.[5] On information and belief, ransomware demands are often resolved for a small fraction of the initial demand amount. For example, a $10 million demand like the one here could resolve for only hundreds of thousands of dollars. Nevertheless, on information and belief, MCNA did not pay any amount to resolve the ransomware demand. On April 7, 2023, LockBit made the stolen data available for download by anyone through its own public-facing website (a "dump site").[6]

6. As a result of MCNA's impermissibly lax data security practices, Plaintiffs and putative class members ("Class Members," defined herein) are at a present and continuing risk for identity and medical identity theft. MCNA compounded this harm by waiting more than two months before notifying affected Customers that their highly sensitive Private Information was now in the hands of sophisticated cybercriminals.

7. It was not until May 26, 2023—eleven weeks after MCNA detected the attack on March 6, 2023—that MCNA began notifying Customers of the Data Breach. MCNA's inexcusable delays permitted the cybercriminals greater access to its servers and prevented Customers from taking immediate defensive measures to protect their valuable Private Information. *See* Exemplar

[3] *Id.* (citing Office of the Maine Atty. Gen., *Data Breach Notifications*, available at https://apps.web.maine.gov/online/aeviewer/ME/40/895b95c8-abc8-41f1-8c3f-b0415575de56.shtml).
[4] *Id.*
[5] *Id.*
[6] *Id.*

Notice Letter, attached hereto as ***Exhibit A***; Kachakech Notice Letter from MCNA and Healthplex, attached hereto as ***Exhibit B*.**

8. The Data Breach was a direct result of MCNA's deficient cybersecurity practices, and the wealth of information and warnings available to MCNA make its failures even more egregious.

9. Taking reasonable, standard precautions against cybercrime and data breaches is a fundamental duty of doing business in the modern age—especially for businesses that profit from analyzing and processing Private Information. By collecting, maintaining, and profiting from Plaintiffs' and Class Members' Private Information, MCNA was required by law to exercise reasonable care and comply with industry and statutory requirements to protect that information—and it failed to do so.

10. Among myriad industry standards and statutes for protection of sensitive information, health care information is specifically governed by federal law under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing regulations. HIPAA requires entities like MCNA to take appropriate technical, physical, and administrative safeguards to secure the privacy of PHI, establishes national standards to protect PHI, and requires timely notice of a breach of unencrypted PHI.

11. Instead, MCNA disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to implement reasonable measures to safeguard its Customers' Private Information and by failing to take necessary steps to prevent unauthorized disclosure of that information. MCNA's woefully inadequate data security measures made the Data Breach a foreseeable, and even likely, consequence of its negligence.

12. MCNA admits that Social Security numbers, driver's licenses, and other

government ID data was taken in the Data Breach. These elements of PII are especially valuable on the dark web and especially likely to be aggregated into dark web databases and subjected to identity theft because they are the documents used to provide proof of identity for all manners of purchase and lease agreements. The trade in forged government identity documents on the dark web is vast, and it is the primary method by which identity thieves obtain both the data and the forged documents that are utilized in identity theft crimes.

13. Further, by aggregating this information obtained from the Data Breach with other sources, or other methods, criminals can assemble a full dossier of Private Information on an individual in order to facilitate a wide variety of frauds, thefts, and scams. Criminals can and do use victims' names, birth dates, Social Security numbers, and addresses to open new financial accounts, incur charges on credit, obtain government benefits and identifications, fabricate identities, and file fraudulent tax returns well before the person whose PII was stolen becomes aware of it.[7] Any one of these instances of identity theft can have devastating consequences for the victim, causing years of often irreversible damage to their credit scores, financial stability, and personal security.

14. Likewise, the exfiltration of PHI puts Plaintiffs and Class Members at a present and continuing risk for medical identity theft, especially in light of the high demand and value of

[7] *See, e.g.*, *Report to Congressional Requesters*, U.S. GOV'T ACCOUNTABILITY OFFICE (June 2007), http://www.gao.gov/assets/270/262899.pdf; Melanie Lockert, *How do hackers use your information for identity theft?*, CREDITKARMA (Oct. 1, 2021), https://www.creditkarma.com/id-theft/i/how-hackers-use-your-information; Ravi Sen, *Here's how much your Private Information is worth to cybercriminals—and what they do with it*, PBS (May 14, 2020), https://www.pbs.org/newshour/science/heres-how-much-your-personal-information-is-worth-to-cybercriminals-and-what-they-do-with-it; Alison Grace Johansen, *4 Lasting Effects of Identity Theft*, LIFELOCK BY NORTON (Feb. 4, 2021), https://lifelock.norton.com/learn/identity-theft-resources/lasting-effects-of-identity-theft.

Medicare identification numbers on the dark web.[8] Medical identity theft poses an even more critical threat to victims—medical fraud could lead to loss of access to necessary healthcare through misuse of paid-for insurance benefits or by incurring substantial medical debt.

15. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, Social Security numbers, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[9]

16. Due to the highly valuable nature of PHI, the FBI has warned healthcare providers that they are likely to be the targets of cyberattacks like the attack that caused the Data Breach.[10]

17. Adding insult to injury, there has been no assurance offered by MCNA that all personal data or copies of data have been recovered or destroyed, or that MCNA has adequately enhanced its security practices or dedicated sufficient resources and staff to avoid a similar breach of its network in the future.

18. Furthermore, as described in detail *infra* ¶¶ 137-41, the known modus operandi of the LockBit ransomware group puts Plaintiffs and Class Members at a much higher likelihood of ongoing risk. LockBit is well known to perform retaliatory "data dumps" of stolen information when corporate victims of its data breach activities refuse to pay their extortion demands. Indeed, they operate a notorious data breach "dump site" on the dark web where they make Plaintiffs' and Class Members' data available to anyone who cares to take it as a method of both punishing those

[8] *What to Know About Medical Identity Theft*, FED. TRADE COMM'N (May 2021), https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft.
[9] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/.
[10] Jim Finkle, *FBI warns healthcare firms they are targeted by hackers*, REUTERS (Aug. 20, 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi-idUSKBN0GK2 4U20140820.

who do not pay and as a means to validate their threats to future victims.

19. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have suffered actual and present injuries, including but not limited to: (a) present and continuing threats of identity theft crimes, fraud, scams, and other misuses of their Private Information; (b) diminution of value of their Private Information; (c) loss of benefit of the bargain (price premium damages); (d) loss of value of privacy and confidentiality of the stolen Private Information; (e) illegal sales of the compromised Private Information; (f) mitigation expenses and time spent on credit monitoring; (g) identity theft insurance costs; (h) "out of pocket" costs incurred due to actual identity theft; (i) credit freezes/unfreezes; (j) expense and time spent on initiating fraud alerts and contacting third parties; (k) decreased credit scores; (l) lost work time; (m) anxiety, annoyance, and nuisance; and (n) continued risk to their Private Information, which remains in MCNA's possession and is subject to further breaches so long as MCNA fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

20. Plaintiffs and Class Members would not have provided their valuable PII and sensitive PHI to MCNA had they known that MCNA would make the Private Information Internet-accessible, not encrypt personal and sensitive data elements such as Social Security numbers, Medicare numbers, health insurance identification numbers, driver's licenses and other government IDs, and dates of birth, and not delete the Private Information it no longer had reason to maintain.

21. Through this lawsuit, Plaintiffs seek to hold MCNA responsible for the injuries it inflicted on Plaintiffs and approximately 8.9 million similarly situated people due to its impermissibly inadequate data security measures, and to seek injunctive relief to ensure the implementation of security measures to protect the Private Information that remains in the

possession of MCNA.

JURISDICTION AND VENUE

22. This Court has original subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d)(2), because the amount in controversy for the Class and State Subclasses exceeds the sum of $5,000,000, exclusive of interest and costs, there are more than 100 Class Members, and minimal diversity exists because many Class Members are citizens of a different state than Defendants.

23. This Court has general personal jurisdiction over Managed Care of North America, Inc. and MCNAIC because their headquarters and principal places of business are in Fort Lauderdale, Florida. This Court has specific personal jurisdiction over Healthplex as to Plaintiff Kachakech and the putative New York Subclass, because Healthplex purposely availed itself of Florida's jurisdiction where Healthplex's customers' Private Information was stored on the systems of Managed Care of North America, Inc. and/or MCNAIC.

24. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), (b)(2), and (c)(2) because a substantial part of the events giving rise to the claims emanated from activities within this District, and MCNA conducts substantial business in this District. In addition, on information and belief, Plaintiffs' and Class Members' Private Information was maintained within this District.

PARTIES

Plaintiff, Agustin Acosta

25. Plaintiff, Agustin Acosta, is, and at all relevant times has been, a resident and citizen of Texas.

26. Plaintiff Acosta receives benefits from MCNA by virtue of his health plan membership.

27. Plaintiff Acosta received a Notice Letter from MCNA dated May 26, 2023, concerning the Data Breach.

28. Since the Data Breach, Plaintiff Acosta has noticed a marked increase in spam texts asking him to respond. He has been experiencing anxiety and stress as a result of the Data Breach and is concerned about how the Data Breach will affect his credit.

29. As a direct and proximate result of the Data Breach, Plaintiff Acosta has made reasonable efforts to mitigate the impact of the Data Breach, including by regularly and closely monitoring his financial accounts.

30. As a result of the Data Breach, Plaintiff Acosta anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. He has faced and faces a present and continuing risk of fraud and identity theft for his lifetime.

Plaintiff, Brittney Brown

31. Plaintiff, Brittney Brown, is, and at all relevant times has been, a resident and citizen of Mississippi.

32. Plaintiff Brown receives benefits from MCNA by virtue of her health plan membership.

33. Plaintiff Brown received a Notice Letter from MCNA dated May 26, 2023, concerning the Data Breach.

34. Since the Data Breach, Plaintiff Brown has received unexplained notifications of activity on her credit line. Plaintiff Brown has also experienced a significant increase in phishing calls and spam text messages since the Data Breach. As a result of the Data Breach, she is fearful and anxious about how the Data Breach will impact her in the future since she does not have

sufficient time to monitor her accounts and cannot afford credit monitoring services.

35. As a direct and proximate result of the Data Breach, Plaintiff Brown has made reasonable efforts to mitigate the impact of the Data Breach, including by regularly and closely monitoring his financial accounts.

36. Plaintiff Brown has faced and faces a present and continuing risk of fraud and identity theft for her lifetime.

Plaintiff, Montwain Carter

37. Plaintiff, Montwain Carter, is, and at all relevant times has been, a resident and citizen of Iowa.

38. Plaintiff Carter receives benefits from MCNA by virtue of his health plan membership.

39. Plaintiff Carter received a Notice Letter from MCNA dated May 26, 2023, concerning the Data Breach.

40. Plaintiff Carter was a victim of identity theft following the Data Breach. After the Data Breach, he was contacted by the Illinois Department of Human Services and told an account had been opened in his name. After the Data Breach, he signed up and paid for an Experian service to monitor his credit, which listed the Illinois Department of Human Services account as a suspicious activity. Also, in October 2023, he had to cancel his credit card due to suspicious charges for Apple Pay, which he did not authorize. He also experienced an increased number of phishing calls and spam text messages since the Data Breach. He is fearful that he will continue to experience identity theft in the future, causing him to lose money and/or take on increased debt, which could negatively affect his credit score. He has experienced increased anxiety as a result of the Data Breach. He is reasonably anxious and fearful that he will be the victim of identity theft or

other fraud in the future because his information was exposed in the Data Breach.

41. As a direct and proximate result of the Data Breach, Plaintiff Carter has made reasonable efforts to mitigate the impact of the Data Breach. He has spent approximately 30 hours monitoring his financial accounts, obtaining credit reports, and signing up for a paid credit monitoring service.

42. As a result of the Data Breach, Plaintiff Carter anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach. He has faced and faces a present and continuing risk of fraud and identity theft for his lifetime.

Plaintiff, Donna Crowe

43. Plaintiff, Donna Crowe, is, and at all relevant times has been, a resident and citizen of Florida.

44. Plaintiff Crowe receives benefits from MCNA by virtue of her health plan membership.

45. Plaintiff Crowe received a Notice Letter from MCNA dated May 26, 2023, concerning the Data Breach.

46. Since the Data Breach, Plaintiff Crowe has experienced an increased number of phishing calls and spam text messages. She is fearful that she will experience identity theft in the future, causing her to lose money and/or take on increased debt, which could negatively affect her credit score. She has experienced increased anxiety as a result of the Data Breach and is anxious and fearful that she will be the victim of identity theft or other fraud in the future because her information was exposed in the Data Breach.

47. As a direct and proximate result of the Data Breach, Plaintiff Crowe has made

reasonable efforts to mitigate the impact of the Data Breach, including calling her credit union regarding the Data Breach and regularly checking her bank and credit card statements for fraud.

48. As a result of the Data Breach, Plaintiff Crowe anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. She has faced and faces a present and continuing risk of fraud and identity theft for her lifetime.

Plaintiff, Shavonne Diggs

49. Plaintiff, Shavonne Diggs, is, and at all relevant times has been, a resident and citizen of Louisiana.

50. Plaintiff Diggs receives benefits from MCNA by virtue of her medical plan membership.

51. Plaintiff Diggs received a Notice Letter from MCNA dated May 26, 2023, concerning the Data Breach.

52. Since the Data Breach, Plaintiff Diggs experienced unauthorized activity on her debit card, and had to cancel the card. She has noticed a marked increase in spam texts asking her to respond, and telephone calls asking her to press a number to continue, which she finds aggravating. She has been experiencing anxiety as a result of the Data Breach and has started meditating and practicing yoga as a result. She is concerned about the violation of her rights, and the risk of identity theft she now faces.

53. As a direct and proximate result of the Data Breach, Plaintiff Diggs has made reasonable efforts to mitigate the impact of the Data Breach, including by regularly and closely monitoring her financial accounts.

54. As a result of the Data Breach, Plaintiff Diggs anticipates spending considerable

time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. Plaintiff Diggs has faced and faces a present and continuing risk of fraud and identity theft for her lifetime.

Plaintiff, Crystal Gannon

55. Plaintiff, Crystal Gannon is, and at all relevant times has been, a resident and citizen of Arkansas.

56. Plaintiff Gannon receives benefits from MCNA by virtue of her health plan membership.

57. Plaintiff Gannon received a Notice Letter from MCNA dated May 26, 2023, concerning the Data Breach.

58. Plaintiff Gannon was a victim of identity theft following the Data Breach. After the Data Breach, she had unauthorized charges on her PayPal and Capital One debit cards linked to bank accounts, requiring that her cards be re-issued. She also experienced an increased number of phishing calls and spam text messages since the Data Breach, including messages that accounts were opened without her authorization and asking her to "Press 1 if you are Crystal Gannon." She is fearful that she will continue to experience identity theft in the future, causing her to lose money and/or take on increased debt, which could negatively affect her credit score. She has received alerts from Credit Karma that said her information is on the dark web. She no longer regularly answers calls on her telephone because of fear of spam calls, and has experienced increased anxiety as a result of the Data Breach. She is reasonably anxious and fearful that she will be the victim of identity theft or other fraud in the future because her information was exposed in the Data Breach.

59. As a direct and proximate result of the Data Breach, Plaintiff Gannon has made reasonable efforts to mitigate the impact of the Data Breach, including by researching the Data

Breach, regularly and closely monitoring her financial accounts, and placing a credit freeze through Experian.

60. As a result of the Data Breach, Plaintiff Gannon anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. She has faced and faces a present and continuing risk of fraud and identity theft for her lifetime.

Plaintiff, Yvon Hanekom

61. Plaintiff, Yvon Hanekom, is, and at all relevant times has been, a resident and citizen of Alabama.

62. Plaintiff Hanekom receives benefits from MCNA by virtue of his health plan membership.

63. Plaintiff Hanekom received a Notice Letter from MCNA dated May 26, 2023, concerning the Data Breach.

64. Plaintiff Hanekom was a victim of medical identity theft following the Data Breach. After the Data Breach, he received a letter from a dentist and another provider regarding a dental claim submitted by an individual not affiliated with him under his dental plan. He has also experienced an increased number of phishing calls and spam text messages since the Data Breach. He is fearful that he will continue to experience identity theft in the future, causing him to lose money and/or take on increased debt, which could negatively affect his credit score. He has experienced increased anxiety as a result of the Data Breach and is anxious and fearful that he will be the victim of identity theft or other fraud in the future because her information was exposed in the Data Breach.

65. As a direct and proximate result of the Data Breach, Plaintiff Hanekom has made

reasonable efforts to mitigate the impact of the Data Breach. He spends nearly an hour per day reviewing his financial accounts for identity theft and fraud. He also reviews his credit report every 2 weeks for suspicious activity. He also spent time requesting a new debit card from his bank after the Data Breach.

66. As a result of the Data Breach, Plaintiff Hanekom anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. He has faced and faces a present and continuing risk of fraud and identity theft for his lifetime.

Plaintiff, Samantha Hathaway

67. Plaintiff, Samantha Hathaway, is, and at all relevant times has been, a resident and citizen of Utah.

68. Plaintiff Hathaway receives benefits from MCNA by virtue of her health plan membership.

69. Plaintiff Hathaway received a Notice Letter from MCNA dated May 26, 2023, concerning the Data Breach.

70. Since the Data Breach, Plaintiff Hathaway has experienced an increased number of phishing calls and spam text messages. She is fearful that she will experience identity theft in the future, causing her to lose money and/or take on increased debt, which could negatively affect her credit score. She has experienced increased anxiety as a result of the Data Breach and is anxious and fearful that she will be the victim of identity theft or other fraud in the future because her information was exposed in the Data Breach.

71. As a direct and proximate result of the Data Breach, Plaintiff Hathaway has made reasonable efforts to mitigate the impact of the Data Breach. She regularly checks all her financial,

health, and insurance accounts. She has also changed the passwords for her financial and other accounts, cancelled her bank and credit cards, and ordered new cards.

72. As a result of the Data Breach, Plaintiff Hathaway anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach. She has faced and faces a present and continuing risk of fraud and identity theft for her lifetime.

Plaintiff, Sara Hughes

73. Plaintiff, Sara Hughes, is, and at all relevant times has been, a resident and citizen of Texas.

74. Plaintiff Hughes receives benefits from MCNA by virtue of her health plan membership.

75. Plaintiff Hughes received a Notice Letter from MCNA dated May 26, 2023 or later, concerning the Data Breach.

76. Since the Data Breach, Plaintiff Hughes had to freeze her debit account and get a new card issued after she noticed fraudulent charges on her account. She has been experiencing anxiety and stress as a result of the Data Breach, which has impacted her physical health. She is concerned about the possibility of identity fraud and the resulting risk to her credit score.

77. As a direct and proximate result of the Data Breach, Plaintiff Hughes has made reasonable efforts to mitigate the impact of the Data Breach, including by subscribing to Credit Karma to monitor her credit reports, and monitoring her financial accounts closely and regularly.

78. As a result of the Data Breach, Plaintiff Hughes anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach. She has faced and faces a present and continuing risk of fraud and identity theft for her

lifetime.

Plaintiff, Tarek Kachakech

79. Plaintiff, Tarek Kachakech, is, and at all relevant times has been, a resident and citizen of New York.

80. Plaintiff Kachakech receives benefits from MCNA Dental and Healthplex by virtue of his health plan membership.

81. Plaintiff Kachakech received a Notice Letter from MCNA Dental and Healthplex dated May 26, 2023, concerning the Data Breach.

82. Since the Data Breach, Plaintiff Kachakech has experienced an increased number of phishing calls and spam text messages. Also, his Facebook account was hacked and subsequently disabled by Facebook. He is anxious and fearful he will continue to experience identity theft in the future because of the Data Breach. He is also suffering emotionally after his Facebook account was hacked because he lost all his contacts and connections.

83. As a direct and proximate result of the Data Breach, Plaintiff Kachakech has made reasonable efforts to mitigate the impact of the Data Breach. He has spent approximately 20 hours reviewing his financial accounts for identity theft and fraud and contacting Facebook regarding the identify theft incident.

84. As a result of the Data Breach, Plaintiff Kachakech anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. He has faced and faces a present and continuing risk of fraud and identity theft for his lifetime.

Plaintiff, Kade McCraw

85. Plaintiff, Kade McCraw, is, and at all relevant times has been, a resident and citizen

of Massachusetts.

86. Plaintiff McCraw receives benefits from MCNA by virtue of his health plan membership.

87. Plaintiff McCraw received a Notice Letter from MCNA dated May 26, 2023, concerning the Data Breach.

88. Plaintiff McCraw was the victim of identity theft following the Data Breach. On or about March 22, 2023, someone attempted to use his Capital One credit card to make a purchase in the amount of $12.48 on Walmart.com. As a result, Capital One had to issue him a new card. He has also experienced an increased number of phishing calls and spam text messages since the Data Breach. He is anxious and fearful that he will continue to experience identity theft in the future because of the Data Breach, causing him to lose money and/or take on increased debt, which could negatively affect his credit score and prevent him from owning a home.

89. As a direct and proximate result of the Data Breach, Plaintiff McCraw has made reasonable efforts to mitigate the impact of the Data Breach. He has spent approximately 10 hours reviewing his financial accounts for identity theft and fraud, researching the Data Breach, reviewing his credit report, and communicating with Capital One regarding the March 22, 2023, identity theft incident. He also spent time obtaining a credit freeze from Experian after the March 22, 2023 identity theft incident. He reviews his credit report periodically for suspicious activity.

90. As a result of the Data Breach, Plaintiff McCraw anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach. He has faced and faces a present and continuing risk of fraud and identity theft for his lifetime.

Plaintiff, Heather Shaffer

91. Plaintiff, Heather Shaffer, is, and since June 2021, has been a resident and citizen of Nebraska.

92. Plaintiff Shaffer received benefits from MCNA by virtue of her health plan membership when she lived in Louisiana.

93. Plaintiff Shaffer received a Notice Letter from MCNA dated May 26, 2023 or later, concerning the Data Breach.

94. Since the Data Breach, Plaintiff Shaffer has noticed a marked increase in phishing emails, spam texts asking her to respond, and telephone calls asking her to press a number to continue. She has received at least one alert from a fraud monitoring product (which she continued subscribing to because of the Data Breach) that someone was trying to access her account. She has been experiencing anxiety and fear of identity theft as a result of the Data Breach, and has seen a psychiatrist for increased anxiety following the Data Breach. She is concerned about the violation of her privacy rights, identity theft, and having to rebuild her credit if that happens.

95. As a direct and proximate result of the Data Breach, Plaintiff Shaffer has made reasonable efforts to mitigate the impact of the Data Breach, including by regularly monitoring her credit reports through Credit Karma and a paid account with Equifax.

96. As a result of the Data Breach, Plaintiff Shaffer anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach. She has faced and faces a present and continuing risk of fraud and identity theft for her lifetime.

Plaintiff, Aliciah Souza-Shores

97. Plaintiff, Aliciah Souza-Shores is, and at all relevant times has been, a resident and

citizen of Louisiana.

98. Plaintiff Souza-Shores receives benefits from MCNA by virtue of her health membership.

99. Plaintiff Souza-Shores received a Notice Letter from MCNA dated May 26, 2023, concerning the Data Breach.

100. Since the Data Breach, Plaintiff Souza-Shores had to close her debit card and open a new one after unauthorized charges appeared on it, has received alerts from Kroll about suspicious activity on her accounts and that her confidential information is on the dark web, and became aware of an attempt to open an account in her name. As a result of the canceled card, she spent considerable time resetting all her automatic payments, including her mortgage payments, and incurred late fees on her mortgage and water bill. In addition, she has noticed inquiries on her credit report that were not initiated by her. Moreover, she has noticed a marked increase in phishing emails, spam texts asking her to respond, and telephone calls asking her to press a number to continue. She has been experiencing anxiety as a result of the Data Breach and spends an hour each day trying to relax and not worry about it. She is concerned about the risk of identity theft and the privacy of her HIPAA-protected information.

101. As a direct and proximate result of the Data Breach, Plaintiff Souza-Shores has made reasonable efforts to mitigate the impact of the Data Breach, including by paying for identity monitoring from Kroll and regularly and closely checking her financial accounts.

102. As a result of the Data Breach, Plaintiff Souza-Shores anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach. She has faced and faces a present and continuing risk of fraud and identity theft for her lifetime.

Plaintiff, Asia Spears

103. Plaintiff, Asia Spears, is, and at all relevant times has been, a resident and citizen of Florida.

104. Plaintiff Spears receives benefits from MCNA by virtue of her health plan membership.

105. Plaintiff Spears received a Notice Letter from MCNA dated May 26, 2023, concerning the Data Breach.

106. Plaintiff Spears was the victim of identity theft following the Data Breach. On or about September 2023, a credit card was opened in her name with a $1,000 credit limit. Additionally, there were several unauthorized transactions in her bank account that caused the account to overdraft by $900. Also, an unauthorized $1,200 transaction appeared on her CashApp. She is out-of-pocket for these losses and the bank closed her account. Plaintiff Spears has also experienced an increased number of phishing calls, emails, and spam text messages since the Data Breach. She is fearful that she will continue to experience identity theft in the future, causing her to lose money and/or take on increased debt, which could negatively affect her credit score. She has experienced increased anxiety as a result of the Data Breach and is anxious and fearful that she will be the victim of identity theft or other fraud in the future because her information was exposed in the Data Breach.

107. As a direct and proximate result of the Data Breach, Plaintiff Spears has made reasonable efforts to mitigate the impact of the Data Breach. She regularly checks her bank accounts for fraud. After the Data Breach, she had to freeze her bank account, change the passwords on her accounts, cancel her debit card, and order a new card.

108. As a result of the Data Breach, Plaintiff Spears anticipates spending considerable

time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach. She has faced and faces a present and continuing risk of fraud and identity theft for her lifetime.

Plaintiff, Heidi Winkler

109. Plaintiff, Heidi Winkler, is, and at all relevant times has been, a resident and citizen of Florida.

110. Plaintiff Winkler receives benefits from MCNA by virtue of her health plan membership.

111. Plaintiff Winkler received a Notice Letter from MCNA dated May 26, 2023, concerning the Data Breach.

112. Plaintiff Winkler was the victim of identity theft following the Data Breach. She had to cancel her debit card and have a new debit card issued due to the card being used for multiple unauthorized purchases. She also experienced fraud when someone tried using her health information to pay for a COVID test. Additionally, a DoorDash account was opened in her name without her authorization. She also noticed an unauthorized charge on her account from a supermarket. She has also experienced an increased number of phishing calls and spam text messages since the Data Breach. She is fearful that she will continue to experience identity theft in the future, causing her to lose money and/or take on increased debt, which could negatively affect her credit score. She has experienced increased anxiety as a result of the Data Breach and is anxious and fearful that she will be the victim of identity theft or other fraud in the future because her information was exposed in the Data Breach.

113. As a direct and proximate result of the Data Breach, Plaintiff Winkler has made reasonable efforts to mitigate the impact of the Data Breach. Dealing with the consequences of the

Data Breach has become a daily occurrence for Plaintiff Winkler, who receives multiple spam calls each day, along with spam text messages. She has spent time addressing the Data Breach, including having to cancel her debit card after it was used for unauthorized purposes.

114. Plaintiff Winkler anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. She has faced and faces a present and continuing risk of fraud and identity theft for her lifetime.

Plaintiff, Franny Zurline

115. Plaintiff, Franny Zurline, is, and at all relevant times has been, a resident and citizen of Idaho.

116. Plaintiff Zurline receives benefits from MCNA by virtue of her health plan membership.

117. Plaintiff Zurline received a Notice Letter from MCNA dated May 26, 2023, concerning the Data Breach.

118. Since the Data Breach, Plaintiff Zurline has experienced an increased number of phishing calls and spam text messages. She is fearful that she will experience identity theft in the future, causing her to lose money and/or take on increased debt, which could negatively affect her credit score. She has experienced increased anxiety as a result of the Data Breach and is anxious and fearful that she will be the victim of identity theft or other fraud in the future because her information was exposed in the Data Breach.

119. As a direct and proximate result of the Data Breach, Plaintiff Zurline has made reasonable efforts to mitigate the impact of the Data Breach, including regularly checking all her financial accounts for fraud.

120. As a result of the Data Breach, Plaintiff Zurline anticipates spending considerable

time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach. She has faced and faces a present and continuing risk of fraud and identity theft for her lifetime.

Defendants

121. Managed Care of North America, Inc. is incorporated and validly existing under the laws of Florida, with its headquarters and principal place of business located at 200 West Cypress Creek Road, Suite 500, Fort Lauderdale, Florida 33309.

122. MCNAIC is incorporated and validly existing under the laws of Texas with its headquarters and principal place of business located at 200 West Cypress Creek Road, Suite 500, Fort Lauderdale, Florida 33309.

123. Healthplex is incorporated and validly existing under the laws of Delaware, with its headquarters and principal place of business located at 333 Earle Ovington Blvd., Suite 300, Uniondale, New York 11553. Healthplex is a wholly owned subsidiary of Managed Care of North America, Inc. or one of its affiliated entities.

FACTUAL ALLEGATIONS

A. MCNA Collects and Uses Personal and Sensitive Customer Data.

124. MCNA "is a leading dental benefits manager committed to providing high quality services to state agencies and managed care organizations for their Medicaid, [CHIP], and Medicare members."[11] MCNA's website defines MCNA Dental as both "MCNA Insurance Company and Managed Care of North America, Inc."[12] MCNA offers dental plans for private

[11] *Company Overview*, MCNA, https://www.mcna.net/en/company-overview (last visited Jan. 20, 2024).
[12] *Id*.

employers, individuals, and families.[13] On information and belief, in some states and at certain times, Managed Care of North America, Inc. contracted with state agencies that administer Medicaid and/or CHIP to provide dental benefits services, and in some states and at certain times, MCNAIC contracted with state agencies that administer Medicaid and/or CHIP to provide dental benefits services. Healthplex is "one of the largest dental administrators in the state of New York with over 3 million members."[14] In 2019, Healthplex was acquired by Managed Care of North America, Inc. or one of its affiliated entities.[15]

125. "MCNA Dental is the largest dental insurer in the nation for government-sponsored Medicaid and CHIP programs" and has "over 5 million members across 8 states."[16]

126. MCNA collects and processes an enormous volume of personal data from millions of Customers, including Private Information like health and patient records, insurance information, and financial information. Some of this information is not provided to MCNA directly, but through Medicaid, CHIP, or Medicare. This personal data is collectively managed and maintained on MCNA computer systems for both MCNA Dental entities and Healthplex whose data was part of the Data Breach.

127. MCNA Dental's website contains a Notice of Privacy Practices, in which it states, "One of our strengths is our ability to administer dental plans in an effective and innovative manner while safeguarding our members' protected health information. . . . "[17] MCNA Dental also claims it is "committed to complying with the requirements and standards of the Health Insurance

[13] *Id*.
[14] *Our History*, HEALTHPLEX, https://www.healthplex.com/about (last visited Jan. 20, 2024).
[15] *See, e.g.*, https://www.prnewswire.com/news-releases/healthplex-acquired-by-affiliates-of-mcna-dental-300920114.html (last visited Jan. 20, 2024).
[16] *Home*, MCNA, https://www.mcna.net/en/home (last visited Nov. 11, 2023).
[17] *Our Privacy Practices*, MCNA, https://www.mcna.net/en/privacy (last visited Jan. 20, 2024).

Portability and Accountability Act of 1996 (HIPAA)."[18] The Notice of Privacy Practices explicitly states it "applies to all MCNA dental programs that are administered by Managed Care of North America, Inc. and MCNA Insurance Company."[19]

128. MCNA Dental states it must follow the privacy practices in its Notice of Privacy Practices, which applied to both Managed Care of North America, Inc. and MCNAIC.[20]

129. MCNA Dental claims to protect PHI, including medical information and other PII like names, addresses, telephone numbers, and Social Security numbers, "in all formats including electronic, written and oral information."[21]

130. MCNA Dental acknowledges that "[t]he law says MCNA has to keep your health information private."[22] It further acknowledges that "[i]n keeping with federal and state laws and our own policy, we have a responsibility to protect the privacy of your information" and that it is "required by law to maintain the privacy and security of your protected health information."[23]

131. MCNA Dental claims it "will not use or share your information other than as described [in the Notice of Privacy Practices] unless you tell us we can in writing."[24] The Notice of Privacy Practices lists several ways that MCNA Dental may use its Customers' information, including, *inter alia*, for research, to comply with the law, and to address workers' compensation claims.[25]

132. MCNA Dental promises to "let you know promptly if a breach occurs that may

[18] *Id.*
[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] *Id.*
[23] *Id.*
[24] *Id.*
[25] *Id.*

have compromised the privacy or security of your information."[26] Notably, the Privacy Policy does not disclose that third parties, who may be reckless and/or negligent, will collect, process, and store PHI protected under HIPAA.

133. MCNA Dental's website touts its proprietary management information system, DentalTrac™, which it uses to manage "enrollment, provider network, claims handling, and other operations data," as "ensur[ing] the security and availability of data through strict adherence to HIPAA requirements, keeping MCNA Dental in full compliance with all federal regulations."[27] MCNA's website also states that "DentalTrac™ is hosted across multiple geographically dispersed, military grade, secure, and state-of-the-art data centers" and that the system "has been based on HIPAA-compliant solutions. MCNA is fully committed to ensuring a clear and easy path to HIPAA readiness well ahead of federally mandated compliance deadlines."[28]

134. Healthplex's Notice of Privacy Practices states: "We are required by law to maintain the privacy and security of your protected health information."[29] Moreover, Healthplex's Financial Information Privacy Notice states it "is committed to maintaining the confidentiality of your personal financial information," defined to include "information about an enrollee or an applicant for health care coverage that identifies the individual, is not generally publicly available, and is collected from the individual or is obtained in connection with providing health care coverage to the individual."[30]

135. Plaintiffs and Class Members relied on MCNA's promise to keep their Private

---

[26] *Id*.
[27] Company Overview, supra n.11.
[28] *Our Technology*, MCNA, https://www.mcna.net/en/technology/ (last visited Nov. 11, 2023).
[29] Notice of Privacy Practices, HEALTHPLEX, available at https://www.healthplex.com/doc/no/F-2507ND (last visited Jan. 20. 2024).
[30] Financial Information Privacy Notice, HEALTHPLEX, available at https://www.healthplex.com/doc/no/F-2507ND (last visited Jan. 20. 2024).

Information confidential and securely maintained, and to only make authorized disclosures of this information. MCNA failed to do so.

136. Plaintiffs and Class Members also relied on MCNA to ensure that it held vendors with whom it shared sensitive Private Information to the same high standards of data protection. MCNA failed to do so.

B. MCNA Allowed the Private Information of Plaintiffs and Class Members to Be Compromised in the Data Breach.

137. According to the Notice of Data Breach posted on its website, MCNA "became aware that an unauthorized party was able to access certain MCNA systems" on March 6, 2023, and that "MCNA subsequently discovered that certain systems within the network may have been infected with malicious code. Through its investigation, MCNA determined that an unauthorized third party was able to access certain systems and remove copies of some personal information between February 26, 2023 and March 7, 2023."[31]

138. In other words, MCNA's investigation revealed that its cyber and data security systems were completely inadequate and allowed cybercriminals to obtain files containing a treasure trove of millions of its Customers' highly sensitive Private Information.

139. The notorious LockBit ransomware gang claimed responsibility for the cyberattack.[32] LockBit is one of the most active ransomware actors, having breached over 1,000

[31] *Notice Letter*, MCNA (May 26, 2023), https://apps.web.maine.gov/online/aeviewer/ME/40/895b95c8-abc8-41f1-8c3f-b0415575de56.shtml (last visited Nov. 11, 2023) (under "Notification and Protection Services" heading, click link titled "MCNA - ME Individual Notice Letters.pdf").

[32] Carly Page, *Ransomware attack on US dental insurance giant exposes data of 9 million patients*, TECHCRUNCH (May 31, 2023), https://techcrunch.com/2023/05/31/ransomware-attack-on-us-dental-insurance-giant-exposes-data-of-9-million-patients/?guccounter=1.

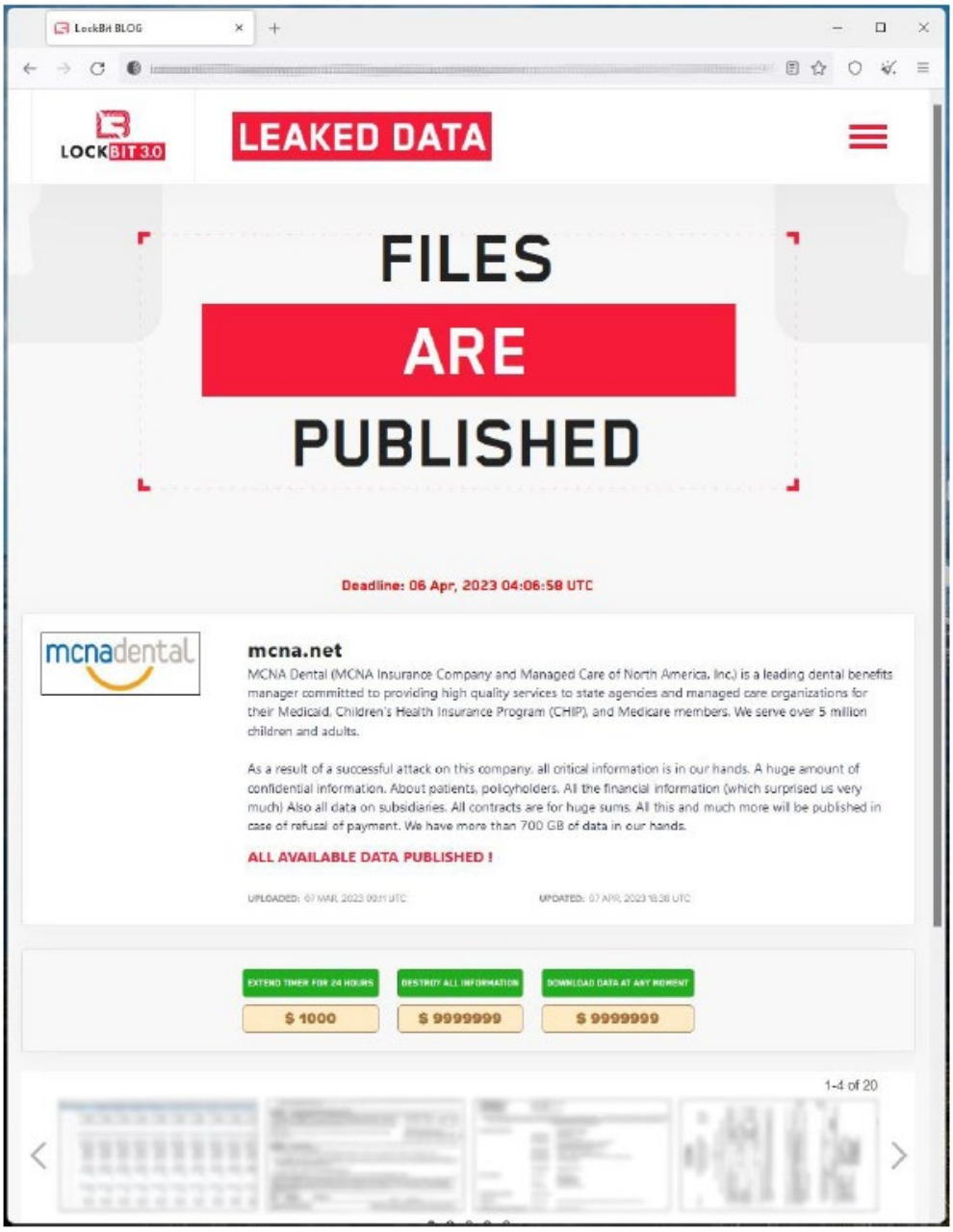
companies worldwide.[33] LockBit is a Russian criminal organization and operates openly. CISA.gov reports that in 2022, LockBit was responsible for 18% of all ransomware attacks in the United States and similar percentages internationally.[34] They have compromised more than 1700 corporations and have dumped the data of all companies that are known to have not paid their ransomware demands onto the dark web for any takers. LockBit's dump site currently contains links to download the data of hundreds of breached companies.

140. MCNA, a self-proclaimed "leader" in the dental benefits industry, knew or should have known of the tactics that groups like LockBit employ.

141. With the Private Information secured and stolen by LockBit, the hackers then purportedly issued a ransom demand to MCNA of $10 million. On information and belief, MCNA refused to negotiate with the hackers or pay the ransom. On April 7, 2023, the presumed deadline of LockBit's ransom demand, LockBit posted over 700 GB of files exfiltrated from the Data Breach on its dump site:

[33] Jeff Stone & Ryan Gallagher, *LockBit Hackers Behind ION Breach Also Hit Royal Mail, Hospital*, BLOOMBERG (Feb. 2, 2023), https://www.bloomberg.com/news/articles/2023-02-02/lockbit-hackers-behind-ion-breach-also-hit-royal-mail-hospital.

[34] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a (last visited Nov. 11, 2023).



142. Data dumped on LockBit's dump site is downloaded by data aggregators aggregated into datasets, and sold on the dark web to various illegal operators, such as identity thieves, payment card duplicators, private information data brokers, and other operators. On information and belief, Plaintiffs' and Class Members' data was posted by LockBit on the dump site and has been exposed for theft and sale on the dark web. This information will remain on the

site indefinitely, causing ongoing risk and continuing harms to plaintiffs.

143. LockBit's history[35] makes the disclosure of Plaintiffs' and Class Members' Private Information to illegal operators a near certainty.[36]

144. Further, the proof data openly published by LockBit proves it has taken far more information from MCNA than MCNA admits in its Notice Letter. LockBit claims (with evidence) that it exfiltrated over 700 GB of data from MCNA, which appears to be most—if not all—of the document data MCNA holds. The proof exhibited by LockBit includes documents regarding employees and Plaintiffs, as well as MCNA's business contracts, tax documents, and all other types of documents a corporation might store. Given the breadth and volume of data taken, it is very likely that (a) MCNA does not know the extent of information taken and (b) the theft includes *all* information MCNA holds regarding Plaintiffs.

C. MCNA's Delay in Securing Its Systems and Notifying Its Customers of the Data Breach Caused Harm to Plaintiffs and Class Members.

145. Although MCNA's systems were first compromised on February 26, 2023, MCNA did not recognize that its servers had been hacked until eight days later, on March 6, 2023.

146. Upon information and belief, MCNA failed to update its systems to include the indicators of compromise or make any mitigation efforts until March 6, 2023, leaving their systems unprotected and open for exploitation for over a week.

147. On May 3, 2023, 58 days after it discovered the theft of its Customers' highly

[35] James Pearson, *Boeing data published by Lockbit hacking gang*, REUTERS (Nov. 10, 2023), https://www.reuters.com/technology/cybersecurity/boeing-data-published-by-lockbit-hacking-gang-2023-11-10/ (last visited Nov. 11, 2023).

[36] "BITWISE SPIDER's LockBit RaaS [Ransomware-as-a-Service] remained the most prolific BGH [Big Game Hunting] operation in 2022 — the adversary's affiliates posted more than 800 victim organizations to the LockBit DLS [Download Site] in 2022." Crowdstrike, *2023 Global Threat Report*, available at https://go.crowdstrike.com/2023-global-threat-report-thank-you.html (last visited Nov. 11, 2023).

sensitive Private Information, MCNA notified the Office of the Maine Attorney General that 8,923,662 individuals were affected by the Data Breach.[37]

148. MCNA also waited well over two months after it discovered its Customers' Private Information had been stolen before sending Notice Letters to individuals whose data was stolen in the Data Breach. While MCNA first sent Notice Letters to impacted individuals on May 26, 2023, Notice Letters to some Plaintiffs were not sent until June 11, 2023 or even later. The Notice Letter stated the following:

> **What happened?**
> On March 6, 2023, MCNA became aware of certain activity in our computer system that happened without our permission. We quickly took steps to stop that activity. We began an investigation right away. A special team was hired to help us. We learned a cybercriminal was able to see and take copies of some information in our computer system between February 26, 2023 and March 7, 2023.
>
> **What information may have been involved?**
> On May 4, 2023, we told the state Medicaid agency that this event may have involved your information. Here is the list of information that was seen and taken:
>
> - Information used to contact you, like first and last name, address, date of birth, telephone number, email
> - Social Security number
> - Driver's license number/other government-issued ID number
> - Health insurance (plan information, insurance company, member number, Medicaid-Medicare ID numbers)
> - Care for teeth or braces (visits, dentist name, doctor name, past care, x-rays/photos, medicines, and treatment)
> - Bills and insurance claims
>
> Some of this information was for a parent, guardian, or guarantor. A guarantor is the person who paid the bill. Information which was seen and taken was not the same for everyone.[38]

149. MCNA's Notice Letter makes no mention the Data Breach involved a ransomware

[37] Office of the Maine Attny. Gen., *Data Breach Notifications: Managed Care of North America, Inc.*, https://apps.web.maine.gov/online/aeviewer/ME/40/895b95c8-abc8-41f1-8c3f-b0415575de56.shtml (last visited Nov. 11, 2023).
[38] Ex. A.

attack, of the ransom demanded by LockBit, or MCNA's refusal to pay even $1.12 per impacted person (or less) to prevent LockBit from publishing Plaintiffs' and Class Members' highly sensitive Private Information.

150. MCNA's Notice Letter also omitted the size and scope of the Data Breach, the ransomware used, or what steps MCNA took or intended to take (if any) to enhance its data security systems and monitoring capabilities to prevent further breaches. Without changes to MCNA's own practices, Plaintiffs' and Class Members' sensitive information remains at risk.

151. MCNA's inadequate communications have left Plaintiffs and Class Members in the dark regarding the extent of the harm they have suffered, and MCNA has demonstrated a pattern of providing inadequate notices and disclosures about the Data Breach.

D. MCNA Knew It Was a Likely Target of a Cyberattack.

152. At all relevant times, MCNA was aware, or reasonably should have been aware, that the Private Information it collected, maintained, and stored in its servers is highly sensitive, susceptible to attack, and could be used for malicious purposes by third parties, such as identity theft, medical identity theft, fraud, and other misuse.

153. The frequency and prevalence of attacks make it imperative for entities to monitor for exploits and attacks routinely and constantly, and regularly update their software and security procedures.

154. MCNA was fully aware the healthcare benefits industry is a prime target for cyber threats.[39] High profile data breaches of similar industry leaders in healthcare put them on notice of this fact, *e.g.*, Trinity Health (3.3 million patients, May 2020); Shields Healthcare Group (2 million patients, March 2022). Between 2020 and 2021, attacks on the healthcare industry increased 71%,

[39] *See* Finkle, *FBI warns healthcare firms they are targeted by hackers*, *supra* n.3.

making it the fifth most common industry targeted by cyberattacks.[40]

E. MCNA Breached Its Duties to Plaintiffs and Class Members.

155. As an entity collecting, maintaining, and profiting from Plaintiffs' and Class Members' highly sensitive Personal Information, MCNA had a duty to exercise reasonable care and comply with applicable industry standards and statutory security requirements to protect their information.

156. Indeed, MCNA was on notice that it was maintaining highly valuable data, which it knew was at risk of being targeted by cybercriminals, and knew of the extensive harm that would occur if Plaintiffs' and Class Members' Private Information was exposed through a data breach.

157. Because Plaintiffs and Class Members provided their Private Information to MCNA, MCNA had a special relationship with Plaintiffs and Class Members which created an independent duty of care. MCNA owed a duty to use reasonable security measures because it undertook to collect, store, and use Customers' Private Information.

158. Despite holding Private Information for millions of individuals, MCNA failed to adopt reasonable data security measures to prevent and detect unauthorized access to their highly sensitive databases, putting their Customers' highly sensitive information at risk.

159. MCNA failed to properly implement data security practices that were reasonable and up to industry standards.

F. MCNA Failed to Comply with Regulatory Requirements and Industry Practices.

160. Federal and state regulators have established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and the healthcare

[40] Check Point Research Team, *Check Point Research: Cyber Attacks Increased 50% Year over Year*, Check Point (Jan. 10, 2022), https://blog.checkpoint.com/security/check-point-research-cyber-attacks-increased-50-year-over-year.

sector. There are a number of state and federal laws, requirements, and industry standards governing the protection of Private Information.

161. For example, at least 24 states have enacted laws addressing data security practices that require businesses that own, license, or maintain Private Information about a resident of that state to implement and maintain "reasonable security procedures and practices" and to protect Private Information from unauthorized access. Florida is one such state and requires that entities like MCNA "take reasonable measures to protect and secure data in electronic form containing personal information." Fla. Stat. § 501.171(2).

162. Additionally, cybersecurity firms have promulgated a series of best practices that at a minimum should be implemented by sector participants including, but not limited to: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting of physical security systems; protecting against any possible communication system; and training staff regarding critical points.[41]

163. The Federal Trade Commission ("FTC") has issued numerous guides for businesses highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making.[42]

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

[41] *See Addressing BPO Information Security: A Three-Front Approach*, DATAMARK, INC. (Nov. 2016), https://insights.datamark.net/addressing-bpo-information-security [https://perma.cc/NY6X-FUY].

[42] *Start With Security*, FED. TRADE COMM'N, at 2, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Nov. 11, 2023).

for business.[43] The guidelines note businesses should protect the personal customer information that they keep; properly dispose of Private Information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

165. The FTC also recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[44]

166. The FTC has brought enforcement actions against businesses for failing to protect customer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

167. The FTC has interpreted Section 5 of the FTC Act to encompass failures to appropriately store and maintain personal data. The body of law created by the FTC recognizes that

---

[43] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N, https://www.ftc.ov/ system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Nov. 11, 2023).

[44] *See Start with Security*, FED. TRADE COMM'N, *supra* n.42.

failure to restrict access to information[45] and failure to segregate access to information[46] may violate the FTC Act.

168. MCNA's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data (*i.e.*, Private Information) constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

169. Furthermore, MCNA is required to comply with the HIPAA Privacy 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. The Privacy Rule and the Security Rule set nationwide standards for protecting health information, including health information stored electronically.

170. The Security Rule requires MCNA to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

[45] *In the Matter of LabMD, Inc.*, Dkt. No. 9357, at 15 ("Procedures should be in place that restrict users' access to only that information for which they have a legitimate need."), https://www.ftc.gov/ system/files/documents/cases/160729labmd-opinion.pdf.
[46] *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 258 (3d Cir. 2015) (stating that companies should use "readily available security measures to limit access between" data storage systems).

d. Ensure compliance by its workforce.[47]

171. Pursuant to HIPAA's mandate that MCNA follow "applicable standards, implementation specifications, and requirements . . . with respect to electronic protected health information," 45 C.F.R. § 164.302, MCNA was required to, at minimum, "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information," 45 C.F.R. § 164.306(e), and "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

172. MCNA is also required to follow the regulations for safeguarding electronic medical information pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. § 17921, 45 C.F.R. § 160.103.

173. Both HIPAA and HITECH obligate MCNA to follow reasonable security standards, respond to, contain, and mitigate security violations, and to protect against disclosure of sensitive patient Private Information. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); 45 C.F.R. § 164.530(f); 42 U.S.C. § 17902.

174. As alleged in this Complaint, MCNA has failed to comply with HIPAA and HITECH. It has failed to maintain adequate security practices, systems, and protocols to prevent data loss, failed to mitigate the risks of a data breach and loss of data, and failed to ensure the confidentiality and protection of PHI.

[47] *Summary of the HIPAA Security Rule*, HHS, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (last visited Nov. 11, 2023).

G. The Data Breach Harmed Plaintiffs and Class Members.

175. MCNA's failure to keep Plaintiffs' and Class Members' Private Information secure has had severe ramifications, examples of which are alleged above for the Plaintiffs. Given the sensitive nature of the information stolen in the Data Breach—names, Social Security numbers, birthdates, addresses, health information—hackers can commit identity theft, financial fraud, and other identity-related fraud against Plaintiffs and Class Members now and into the indefinite future.

176. This data is highly coveted and valuable on underground or black markets. Upon information and belief, Plaintiffs' and Class Members' data has already been leaked and sold on the black market.

177. Cyber criminals sell health information at a far higher premium than stand-alone PII. This is because health information enables thieves to go beyond traditional identity theft and obtain medical treatments, purchase prescription drugs, submit false bills to insurance companies, or even undergo surgery under a false identity.[48] The shelf life for this information is also much longer—while individuals can update their credit card numbers, they are less likely to change their Medicare numbers, health insurance information, or Social Security numbers.

178. Medicare beneficiary numbers like Plaintiffs' are "even more valuable than stolen credit cards," and often result in the filing of false claims for Medicare reimbursement.[49]

179. According to the U.S. Government Accountability Office, "stolen data may be held

[48] *Medical Identity Theft: FAQs for Health Care Providers and Health Plans*, FTC, https://www.ftc.gov/system/files/documents/plain-language/bus75-medical-identity-theft-faq-health-care-health-plan.pdf (last visited Nov. 11, 2023).

[49] Melissa D. Berry, *Medicare under attack: Healthcare data breaches increase fraud risks*, THOMSON REUTERS (Mar. 3, 2023), https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/medicare-fraud-risks.

for up to a year or more before being used to commit identity theft," and "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years."[50]

180. Because of its value and the loss of sensitive health information and Social Security numbers, future identity theft is imminently and certainly impending.

181. The exposure of any Private Information can cause unexpected harms one would not ordinarily associate with the type of information stolen. Cybercriminals routinely aggregate Private Information from multiple illicit sources and use stolen information to gather even more information through social engineering, credential stuffing, and other methods. The resulting complete dossiers of Private Information are particularly prized among cybercriminals because they expose the target to every manner of identity theft and fraud.

182. Identity thieves can use Private Information such as that exposed in the Data Breach to: (a) apply for credit cards or loans; (b) purchase prescription drugs or other medical services; (c) commit immigration fraud; (d) obtain a fraudulent driver's license or ID card in the victim's name; (e) obtain fraudulent government benefits or insurance benefits; (f) file a fraudulent tax return using the victim's information; (g) commit espionage; or (h) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during an arrest.

183. Annual monetary losses for victims of identity theft are in the billions of dollars. In 2017, fraudsters stole $16.8 billion from consumers in the United States, which includes $5.1

[50] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO-07-737, U.S. GOV'T ACCOUNTABILITY OFF., at 42 (June 2007), https://www.govinfo.gov/content/pkg/GAOREPORTS-GAO-07737/html/GAO REPORTSGAO-07-737.htm (last visited Nov. 11, 2023).

billion stolen through bank account take-overs.[51]

184. The annual cost of identity theft is even higher. McAfee and the Center for Strategic and International Studies estimates that the likely annual cost to the global economy from cybercrime is $445 billion a year.[52]

185. For Plaintiffs and Class Members who had their Social Security numbers exposed, the unauthorized disclosure can be particularly damaging because, unlike a credit card, Social Security numbers cannot easily be replaced. Furthermore, as the Social Security Administration warns:

> Keep in mind that a new number probably won't solve all your problems. This is because other governmental agencies (such as the Internal Revenue Service and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other Private Information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other Private Information, such as your name and address, remains the same.
>
> If you receive a new Social Security number, you shouldn't use the old number anymore.

For some victims of identity theft, a new number actually creates new problems. If the old credit card information is not associated with the new number, the absence of any credit history under the new number may make it more difficult to get credit.[53]

186. Reimbursing a consumer for a financial loss due to fraud does not make that

---

[51] *2018 Identity fraud: Fraud Enters a New Era of Complexity*, JAVELIN, https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity (last visited Nov. 11, 2023).

[52] *Facts + Statistics: Identity theft and cybercrime*, INSURANCE INFORMATION INSTITUTE, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last visited Nov. 11, 2023).

[53] *Identity Theft and Your Social Security Number*, SOCIAL SEC. ADMIN., http://www.ssa.gov/pubs/10064.html (last visited Nov. 11, 2023).

individual whole again. On the contrary, in addition to the irreparable damage that may result from the theft of a Social Security number, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.

187. Moreover, cybercriminals need not harvest Plaintiffs' and Class Members' Social Security numbers in order to commit identity fraud or misuse their Private Information. Cybercriminals can cross-reference the data stolen from the Data Breach and combine it with other sources to create "Fullz" packages, which can then be used to commit fraudulent activity on Plaintiffs' and Class Members' financial accounts.

188. And, the impact of identity theft can have ripple effects, which can adversely affect the future financial trajectories of victims' lives. For example, the Identity Theft Resource Center reports that respondents to their surveys in 2013-2016 described that the identity theft they experienced affected their ability to get credit cards and obtain loans such as student loans or mortgages.[54] For some victims, this could mean the difference between going to college or not, becoming a homeowner or not, or having to take out a high interest payday loan versus a lower-interest loan.

189. It is no wonder then that identity theft exacts a severe emotional toll on its victims.

190. The 2017 Identity Theft Resource Center survey[55] evidences the emotional suffering experienced by victims of identity theft:

---

[54] *Identity Theft: The Aftermath 2017*, IDENTITY THEFT RESOURCE CENTER, https://www.idtheftcenter.org/wp-content/uploads/images/page-docs/Aftermath_2017.pdf (last visited Nov. 11, 2023).

[55] *Id*.

- 75% of respondents reported feeling severely distressed;
- 67% reported anxiety;
- 66% reported feelings of fear related to personal financial safety;
- 37% reported fearing for the financial safety of family members;
- 24% reported fear for their physical safety;
- 15.2% reported a relationship ended or was severely and negatively impacted by identity theft; and
- 7% reported feeling suicidal.

191. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances;
- 37.1% reported an inability to concentrate / lack of focus;
- 28.7% reported they were unable to go to work because of physical symptoms;
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues); and
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[56]

192. There may also be a significant time lag between when Private Information is stolen and when it is actually misused. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting

[56] *Id*.

from data breaches cannot necessarily rule out all future harm.[57]

193. As the result of the Data Breach, Plaintiffs and Class Members have suffered and/or will suffer or continue to suffer economic loss, a substantial risk of future identity theft, and other actual harm for which they are entitled to damages, including, but not limited to, the following:

- losing the inherent value of their Private Information;
- losing the value of MCNA's implicit promises of adequate data security;
- identity theft and fraud resulting from the theft of their Private Information;
- costs associated with the detection and prevention of identity theft and unauthorized use of their medical and health insurance information;
- costs associated with purchasing credit monitoring and identity theft protection services;
- unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;
- lowered credit scores resulting from credit inquiries following fraudulent activities;
- costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised

[57] *See Report to Congressional Requesters*, U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* n.7.

accounts, and the stress, nuisance and annoyance of dealing with the repercussions of the Data Breach; and

- the continued imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Private Information being in the possession of one or many unauthorized third parties.

194. Additionally, Plaintiffs and Class Members place significant value in data security.

195. Because of the value consumers place on data privacy and security, companies with robust data security practices can command higher prices than those who do not. Indeed, if consumers did not value their data security and privacy, companies like MCNA would have no reason to tout their data security efforts to their actual and potential Customers.

196. Consequently, had Customers, including Plaintiffs and Class Members, known the truth about MCNA's data security practices—that the company would not adequately protect and store their data—they would not have entrusted their Private Information with MCNA, purchased health benefits that included MCNA's services, or paid as much for such services or benefits. As such, Plaintiffs and Class Members did not receive the benefit of their bargain with MCNA because they paid for a value of services they expected but did not receive.

197. When MCNA announced the Data Breach to its Customers, it deliberately underplayed the Data Breach's severity, obfuscated the nature of the Data Breach, and offered only *de minimis* relief. MCNA merely offered its Customers 12 months of free identity theft protection service and told them to "check your bills and accounts to be sure they look correct." [58] Not only are these suggestions steps that Plaintiffs and Class Members must take on their own free time, but they fail to compensate Plaintiffs and Class Members for the lifetime risks they face.

[58] *See* Ex. A.

198. One year of complimentary identity theft protection services to victims does not adequately address the lifelong harm that Plaintiffs and Class Members will face following the Data Breach. Indeed, the Data Breach involves Private Information that cannot be changed, such as Social Security numbers and PHI.

199. Plaintiffs themselves suffered incidences of harm, including identity theft, which are alleged herein in detail.

CLASS ACTION ALLEGATIONS

200. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as appropriate, and (c)(4), Plaintiffs seek certification of the following nationwide class (the "Class" or the "Nationwide Class"):

Nationwide Class

> **All persons in the United States whose Private Information was compromised in the Data Breach reported to have occurred on or about February 26, 2023.**

201. The Nationwide Class asserts claims against MCNA for negligence (Count I); negligence per se (Count II); breach of implied contract (Count III); unjust enrichment (Count IV); and for declaratory and injunctive relief under the Declaratory Judgment Act, 28 U.S.C. §§ 2201 *et seq.* (Count V).

202. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as appropriate, and (c)(4), Plaintiffs seek certification of state common law claims in the alternative to the nationwide claims, as well as statutory claims under state data breach statutes and/or consumer protection on behalf of subclasses for residents of Alabama, Arkansas, Florida, Idaho, Iowa, Louisiana, Massachusetts, Mississippi, Nebraska, New York, Texas, and Utah (collectively "State Subclasses" or individually "State Subclass"). Each State Subclass is defined as follows:

Alabama Subclass

All residents of Alabama whose Private Information was compromised in the Data Breach reported to have occurred on or about February 26, 2023.

Arkansas Subclass

All residents of Arkansas whose Private Information was compromised in the Data Breach reported to have occurred on or about February 26, 2023.

Florida Subclass

All residents of Florida whose Private Information was compromised in the Data Breach reported to have occurred on or about February 26, 2023.

Idaho Subclass

All residents of Idaho whose Private Information was compromised in the Data Breach reported to have occurred on or about February 26, 2023.

Iowa Subclass

All residents of Iowa whose Private Information was compromised in the Data Breach reported to have occurred on or about February 26, 2023.

Louisiana Subclass

All residents of Louisiana whose Private Information was compromised in the Data Breach reported to have occurred on or about February 26, 2023.

Massachusetts Subclass

All residents of Massachusetts whose Private Information was compromised in the Data Breach reported to have occurred on or about February 26, 2023.

Mississippi Subclass

All residents of Mississippi whose Private Information was compromised in the Data Breach reported to have occurred on

or about February 26, 2023.

Nebraska Subclass

All residents of Nebraska whose Private Information was compromised in the Data Breach reported to have occurred on or about February 26, 2023.

New York Subclass

All residents of New York whose Private Information was compromised in the Data Breach reported to have occurred on or about February 26, 2023.

Texas Subclass

All residents in Texas whose Private Information was compromised the Data Breach reported to have occurred on or about February 26, 2023.

Utah Subclass

All residents in Utah whose Private Information was compromised the Data Breach reported to have occurred on or about February 26, 2023.

203. Excluded from the Nationwide Class and the State Subclasses (collectively, the "Classes") are MCNA, any entity in which MCNA has a controlling interest, and MCNA's officers, directors, legal representatives, successors, subsidiaries, and assigns; all federal, state, or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; any judicial officer presiding over any aspect of this matter, members of their immediate family, and members of their judicial staff; any individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; Plaintiffs' counsel and MCNA's counsel; members of the jury; and the legal representatives.

204. Plaintiffs hereby reserve the right to amend or modify the definitions of the Classes with greater specificity or division after having had an opportunity to conduct discovery.

205. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Classes are so numerous and geographically dispersed that the joinder of all members is impractical. While the exact number of Class Members is unknown to Plaintiffs at this time, MCNA has acknowledged that the Private Information of at least 8,923,662 individuals throughout the United States was compromised in the Data Breach. Those persons' names and addresses are available from MCNA's records, and Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include electronic mail, U.S. Mail, internet notice, and/or published notice. Upon information and belief, there are at least thousands of members in each State Subclass, making joinder of all State Subclass Members impractical.

206. **Predominance of Common Issues**. **Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Rule 23(a)(2)'s commonality requirement and Rule 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class Members. The common questions include:

a. Whether MCNA unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

b. Whether MCNA's conduct violated the FTC Act and/or HIPAA;

c. Whether MCNA's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including HIPAA and HITECH;

d. Whether MCNA's data security systems were consistent with industry

standards;

e. Whether MCNA knew or should have known that its servers and configurations were vulnerable to attack;

f. Whether MCNA failed to take adequate and reasonable measures to ensure that its computer, applications, and data systems were protected and updated;

g. Whether MCNA failed to take available steps to prevent and stop the Data Breach from happening;

h. Whether MCNA should have discovered the Data Breach earlier;

i. Whether MCNA took reasonable measures to determine the extent of the Data Breach after it was discovered;

j. Whether MCNA owed tort duties to Plaintiffs and Class Members to protect their Private Information;

k. Whether MCNA owed a duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

l. Whether MCNA's delay in informing Plaintiffs and Class Members of the Data Breach was unreasonable;

m. Whether MCNA's method of informing Plaintiffs and Class Members of the Data Breach was unreasonable;

n. Whether MCNA breached their duties to protect the Private Information of Plaintiffs and Class Members by failing to provide adequate data security;

o. Whether MCNA's failure to secure Plaintiffs' and Class Members' Private Information in the manner alleged violated federal, state, and local laws, and/or industry standards;

p. Whether MCNA's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach, resulting in the unauthorized access to and/or theft of Plaintiffs' and Class Members' Private Information;

q. Whether MCNA has an implied contractual obligation to use reasonable security measures and whether it complied with such contractual obligation;

r. Whether MCNA's conduct amounted to violations of state consumer protection statutes;

s. Whether, as a result of MCNA's conduct, Plaintiffs and Class Members face a significant ongoing threat of identity theft, harm, and/or have already suffered harm, and, if so, the appropriate measure of damages to which they are entitled;

t. Whether MCNA should retain the money paid by Plaintiffs and Class Members to protect their Private Information;

u. Whether MCNA should retain Plaintiffs' and Class Members' valuable Private Information; and

v. Whether, as a result of MCNA's conduct, Plaintiffs and Class Members are entitled to injunctive, equitable, declaratory, and/or other relief, and, if so, the nature of such relief.

207. **Typicality. Fed. R. Civ. P. 23(a)(3).** As to each of the Classes, Plaintiffs' claims are typical of other Class Members' claims because Plaintiffs and Class Members were subjected to the same allegedly unlawful conduct and damaged in the same way. Plaintiffs' Private Information was in MCNA's possession at the time of the Data Breach and was compromised as a result of the Data Breach. Plaintiffs' damages and injuries are akin to those of other Class Members and Plaintiffs seek relief consistent with the relief of the Classes.

208. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiffs are adequate representatives of the Classes because Plaintiffs are each members of the Nationwide Class, and respectively members of the State Subclasses, and are committed to pursuing this matter against MCNA to obtain relief for the Classes. Plaintiffs have no conflicts of interest with the Classes. Plaintiffs' Counsel are competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the interests of all the Classes.

209. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to Plaintiffs and Class Members may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiffs and Class Members are relatively small compared to the burden and expense required to individually litigate their claims against MCNA, and thus, individual litigation to redress MCNA's wrongful conduct would be impracticable. Individual litigation by each Class Member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

210. **Manageability**. **Fed. R. Civ. P. 23(b)(3).** The litigation of the class claims alleged herein is manageable. MCNA's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates there would be no significant

manageability problems with prosecuting this lawsuit as a class action.

211. **Ascertainability**. All members of the proposed Classes are readily ascertainable. The Classes are defined by reference to objective criteria, and there is an administratively feasible mechanism to determine who fits within the Classes. MCNA has access to information regarding which individuals were affected by the Data Breach and has already provided notifications to some of those people. Using this information, the members of the Classes can be identified, and their contact information ascertained for purposes of providing notice to the Classes.

212. **Particular Issues. Fed. R. Civ. P. 23(c)(4).** Particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether MCNA owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether MCNA breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether MCNA failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between MCNA on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether MCNA breached the implied contract;

f. Whether MCNA adequately and accurately informed Plaintiffs and Class Members their Private Information had been compromised;

g. Whether MCNA failed to implement and maintain reasonable security

procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether MCNA engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiffs and Class Members; and

i. Whether Class Members are entitled to actual, consequential, statutory, and/or nominal damages, and/or injunctive relief as a result of MCNA's wrongful conduct.

213. **Injunctive and Declaratory Relief. Fed. R. Civ. P. 23(b)(2) and (c).** Finally, class certification is also appropriate under Rule 23(b)(2) and (c). MCNA, through its uniform conduct, acted or refused to act on grounds generally applicable to the Classes as a whole, making injunctive and declaratory relief appropriate to the Classes as a whole, including:

a. Ordering MCNA to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

b. Ordering that, to comply with MCNA's explicit or implicit contractual obligations and duties of care, MCNA must implement and maintain reasonable security and monitoring measures, including, but not limited to:

i. prohibiting MCNA from engaging in the wrongful and unlawful acts alleged herein;

ii. requiring MCNA to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring MCNA to delete and purge the Private Information of Plaintiffs and Class Members unless MCNA can provide to the Court reasonable justification for the retention and use of such information when weighed against the

privacy interests of Plaintiffs and Class Members;

iv. requiring MCNA to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiffs' and Class Members' Private Information;

v. requiring MCNA to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on MCNA's systems on a periodic basis;

vi. prohibiting MCNA from maintaining Plaintiffs' and Class Members' Private Information on a cloud-based database until proper safeguards and processes are implemented;

vii. requiring MCNA to segment data by creating firewalls and access controls so that, if one area of MCNA's network is compromised, hackers cannot gain access to other portions of MCNA's systems;

viii. requiring MCNA to conduct regular database scanning and securing checks;

ix. requiring MCNA to monitor ingress and egress of all network traffic;

x. requiring MCNA to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling Private Information, as well as protecting the Private Information of Plaintiffs and Class Members;

xi. requiring MCNA to implement a system of tests to assess its

respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with MCNA's policies, programs, and systems for protecting personal identifying information;

xii. requiring MCNA to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor MCNA's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated;

xiii. requiring MCNA to meaningfully educate all Class Members about the threats that it faces because of the loss of its confidential Private Information to third parties, as well as the steps affected individuals must take to protect themselves; and

xiv. Incidental retrospective relief, including but not limited to restitution.

CAUSES OF ACTION

ON BEHALF OF THE NATIONWIDE CLASS, OR ALTERNATIVELY, ON BEHALF OF THE STATE SUBCLASSES, AND AS TO ALL DEFENDANTS

COUNT I
NEGLIGENCE

214. Plaintiffs reallege and incorporate by reference the allegations contained in paragraphs 1 through 213 above, as if fully set forth herein.

215. MCNA collected sensitive Private Information from Plaintiffs and Class Members as a requirement for using MCNA's products and services.

216. MCNA owed a duty to Plaintiffs and Class Members to exercise reasonable care in

obtaining, retaining, securing, safeguarding, deleting, and protecting their Private Information in its possession from being compromised, lost, stolen, accessed, or misused by unauthorized persons.

217. More specifically, this duty included, among other things: (a) regularly designing, maintaining, and testing MCNA's security systems to ensure that Plaintiffs' and Class Members' Private Information in MCNA's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards, including regularly updating, patching, and evaluating security measures.

218. MCNA's duty to use reasonable care arose from several sources, including but not limited to those alleged herein.

219. MCNA had common law duties to prevent foreseeable harm to Plaintiffs and Class Members. These duties existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices.

220. MCNA's duty to use reasonable security measures also arose as a result of the special relationship that existed between MCNA, on the one hand, and Plaintiffs and Class Members, on the other hand. The special relationship arose because Plaintiffs and Class Members provided their valuable PII and sensitive PHI to MCNA. Only MCNA could have ensured that its security systems and data storage architecture were sufficient to prevent or minimize the Data Breach because it had exclusive knowledge and control regarding same.

221. MCNA admits that it has a responsibility to protect consumer data, that it is entrusted with this data, and that it did not live up to its responsibility to protect the Private

Information at issue here. Discovery is necessary to fully understand the reasons for this failure, but it appears that in its quest for rapid growth over the last three years, MCNA has failed to put adequate resources and emphasis on the need for data security.

222. MCNA knew or should have known that its computing systems and data storage architecture were vulnerable to unauthorized access and targeting by hackers for the purpose of stealing and misusing confidential Private Information.

223. MCNA also had a duty to safeguard the Private Information of Plaintiffs and Class Members and to promptly notify them of a breach because of state laws and statutes that require MCNA to reasonably safeguard sensitive Private Information, as detailed herein.

224. Timely, adequate notification was required, appropriate, and necessary so that, among other things, Plaintiffs and Class Members could take appropriate measures to freeze or lock their credit profiles; avoid unauthorized charges to their credit or debit card accounts; cancel or change usernames and passwords on compromised accounts; monitor their account information and credit reports for fraudulent activity; contact their banks or other financial institutions that issue their credit or debit cards; obtain credit monitoring services; contact their health insurers or governmental health insurance providers; and take other steps to mitigate or ameliorate the damages caused by MCNA's misconduct. MCNA was the only entity that had sufficient knowledge to properly provide this notice.

225. MCNA breached the duties it owed to Plaintiffs and Class Members alleged above and, thus, was negligent in failing to do so. MCNA breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the Private Information of Plaintiffs and Class Members; (b) detect the Data Breach while it was ongoing; (c) maintain security systems consistent with industry

standards during the period of the Data Breach; (d) comply with regulations protecting the Private Information at issue during the period of the Data Breach; and (e) disclose in a timely and adequate manner that Plaintiffs' and Class Members' Private Information in MCNA's possession had been or was reasonably believed to have been, stolen, or compromised.

226. But for MCNA's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, their Private Information would not have been compromised.

227. MCNA's failure to take proper security measures to protect the sensitive Private Information of Plaintiffs and Class Members created conditions conducive to a foreseeable, intentional act, namely the unauthorized access of Plaintiffs' and Class Members' Private Information.

228. Plaintiffs and Class Members were foreseeable victims of MCNA's inadequate data security practices, and it was also foreseeable that MCNA's failure to provide timely and adequate notice of the Data Breach would result in injury to Plaintiffs and Class Members as alleged in this Complaint.

229. As a direct and proximate result of MCNA's negligence, Plaintiffs and Class Members have been injured and are entitled to compensatory and consequential damages suffered because of the Data Breach in an amount to be proven at trial.

230. Such injuries include one or more of the following: (a) actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; (b) the loss of the value of their privacy and the confidentiality of the stolen Private Information; (c) the illegal sale of the compromised Private Information on the black market; (d) the present and continuing threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; (e) mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes

and unfreezes; (f) the time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; (g) the expenses incurred and time spent initiating fraud alerts; (h) the resulting decrease in credit scores and ratings; (i) their lost work time; (j) the lost value of the Private Information; (k) the lost value of access to their Private Information permitted by MCNA; (l) the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of MCNA's Data Breach; (m) lost benefit of their bargains and overcharges for services or products; and (n) the nominal and general damages and other economic and non-economic harm suffered.

COUNT II
NEGLIGENCE *PER SE*

231. Plaintiffs reallege and incorporate by reference the allegations contained in paragraphs 1 through 213 above, as if fully set forth herein.

232. As alleged above, MCNA had duties arising under HIPAA, the HIPAA Privacy Rule and Security Rule, HITECH, and the FTC Act.

233. MCNA's violation of HIPAA, the HIPAA Privacy Rule and Security Rule, HITECH, and Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

234. Plaintiffs and Class Members are consumers within the class of persons that HIPAA, HITECH, and Section 5 of the FTC Act were intended to protect.

235. The harm that has occurred is the type of harm HIPAA, HITECH, and the FTC Act were intended to guard against.

236. The FTC has pursued enforcement actions against businesses and healthcare entities that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

237. MCNA breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

238. In addition, under state data security and consumer protection statutes such as those outlined herein, MCNA had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs' and Class Members' Private Information.

239. Plaintiffs and Class Members were foreseeable victims of MCNA's violations of HIPAA, HITECH, and the FTC Act, and state data security and consumer protection statutes. MCNA knew or should have known that its failure to implement reasonable data security measures to protect and safeguard Plaintiffs' and Class Members' Private Information would cause damage to Plaintiffs and the Class.

240. But for MCNA's violations of these applicable laws and regulations, Plaintiffs' and Class Members' Private Information would not have been accessed and exfiltrated by unauthorized cybercriminals.

241. As a direct and proximate result of MCNA's negligence *per se*, Plaintiffs and Members have been injured and are entitled to compensatory and consequential damages suffered because of the Data Breach in an amount to be proven at trial. Such injuries include one or more of the following: (a) actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; (b) the loss of the value of their privacy and the confidentiality of the stolen Private Information; (c) the illegal sale of the compromised Private Information on the black market; (d) the ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; (e) the mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; (f) the time

spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; (g) the expenses incurred and time spent initiating fraud alerts; (h) the resulting decrease in credit scores and ratings; (i) their lost work time; (j) the lost value of the Private Information; (k) the lost value of access to their Private Information permitted by MCNA; (l) the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of MCNA's Data Breach; (m) the lost benefit of their bargains and overcharges for services or products; and (n) nominal and general damages; and other economic and non-economic harm.

COUNT III
BREACH OF IMPLIED CONTRACT AND BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING

242. Plaintiffs reallege and incorporate by reference the allegations contained in paragraphs 1 through 213 above, as if fully set forth herein.

243. MCNA offered to provide services to its Customers, including Plaintiffs and Class Members, in exchange for payment.

244. MCNA also required Plaintiffs and Class Members to provide it with their Private Information in order to receive services.

245. In turn, MCNA impliedly promised to protect Plaintiffs' and Class Members' Private Information through adequate data security measures.

246. Plaintiffs and Class Members accepted MCNA's offer by providing their valuable PII and sensitive PHI to MCNA and their respective providers who in turn provided that information to MCNA in exchange for Plaintiffs and Class Members receiving MCNA's services, and then by paying for and receiving the same.

247. Plaintiffs and Class Members would not have done the foregoing but for the above-

described agreement with the company.

248. A meeting of the minds occurred when Plaintiffs and Class Members agreed to, and did, provide their Private Information to MCNA in exchange for, amongst other things, the protection of such information.

249. Plaintiffs and Class Members fully performed their obligations under the implied contracts with MCNA.

250. However, MCNA breached the implied contracts it made with Plaintiffs and Class Members by failing to safeguard and protect their Private Information and by failing to provide timely and accurate notice to them that their Private Information was compromised as a result of the Data Breach.

251. MCNA further breached the implied contracts with Plaintiffs and Class Members by failing to comply with its promise to abide by HIPAA.

252. MCNA further breached the implied contracts with Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information MCNA created, received, maintained, and transmitted in violation of 45 C.F.R. § 164.306(a)(1).

253. MCNA further breached the implied contracts with Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1).

254. MCNA further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. § 164.306(a)(2).

255. In sum, Plaintiffs and Class Members have performed under the relevant agreements, or such performance was waived by the conduct of MCNA.

256. Moreover, the covenant of good faith and fair dealing is an element of every contract. All such contracts impose on each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract along with its form.

257. MCNA's conduct as alleged herein also violated the implied covenant of good faith and fair dealing inherent in every contract.

258. As a direct and proximate result of MCNA's above-alleged breach of implied contract, Plaintiffs and Class Members have suffered (and will continue to suffer): (a) actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; (b) the loss of the value of their privacy and the confidentiality of the stolen Private Information; (c) the illegal sale of the compromised Private Information on the black market; (d) the ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; (e) the mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; (f) the time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; (g) the expenses incurred and time spent initiating fraud alerts; (h) the resulting decrease in credit scores and ratings; (i) their lost work time; (j) the lost value of the Private Information; (k) the lost value of access to their Private Information permitted by MCNA; (l) the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of MCNA's Data Breach; (m) the lost benefit of

their bargains and overcharges for services or products; and (n) nominal and general damages; and other economic and non-economic harm.

259. Accordingly, Plaintiffs and the Class are entitled to damages in an amount to be determined at trial, including actual, consequential, and nominal damages, along with costs and attorneys' fees incurred in this action.

COUNT IV
UNJUST ENRICHMENT

260. Plaintiffs reallege and incorporate by reference the allegations contained in paragraphs 1 through 213 above, as if fully set forth herein.

261. This Count is pled in the alternative to Plaintiffs' claim for breach of implied contract (Count III).

262. Plaintiffs and Class Members have an interest, both equitable and legal, in the Private Information about them that was conferred upon, collected by, and maintained by MCNA, and that was ultimately stolen in the Data Breach.

263. MCNA benefitted by the conferral upon it of the Private Information pertaining to Plaintiffs and Class Members and by its ability to retain, use, sell, and profit from that information. MCNA understood that it so benefitted.

264. MCNA also understood and appreciated that Plaintiffs' and Class Members' Private Information was in fact private and confidential, and its value depended upon MCNA maintaining the privacy and confidentiality of that Private Information.

265. But for MCNA's willingness and commitment to maintain its privacy and confidentiality, Plaintiffs and Class Members would not have provided their Private Information to MCNA.

266. Because of its use of Plaintiffs' and Class Members' Private Information, MCNA

sold more services and products than it otherwise would have. MCNA was unjustly enriched by profiting from the additional services and products it was able to market, sell, and create to the detriment of Plaintiffs and Class Members.

267. MCNA also benefitted through its unjust conduct by retaining money that it should have used to provide reasonable and adequate data security to protect Plaintiffs' and Class Members' Private Information.

268. MCNA further benefited through its unjust conduct in the form of the profits it gained through the use of Plaintiffs' and Class Members' Private Information.

269. The benefits conferred upon, received, and enjoyed by MCNA were not conferred officiously or gratuitously. Under the circumstances, it would be inequitable, unfair, and unjust for MCNA to retain these wrongfully obtained benefits. MCNA's retention of wrongfully obtained monies would also violate fundamental principles of justice, equity, and good conscience.

270. As a result of MCNA's wrongful conduct as alleged in this Complaint (including, among things, its failure to employ adequate data security measures; its continued maintenance and use of the Private Information belonging to Plaintiffs and Class Members without having adequate data security measures; and its other conduct facilitating the theft of that Private Information), MCNA has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and Class Members.

271. MCNA's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiffs' and Class Members' sensitive Private Information, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

272. MCNA's defective security and its unfair and deceptive conduct have, among other

things, caused Plaintiffs and Class Members to unfairly incur substantial time and/or costs to mitigate and monitor the use of their Private Information and has caused the Plaintiffs and Class Members other damages as alleged herein.

273. Plaintiffs have no adequate remedy at law.

274. MCNA is therefore liable to Plaintiffs and Class Members for restitution or disgorgement in the amount of the benefit conferred on MCNA as a result of its wrongful conduct, including specifically: (a) the value to MCNA of the Private Information that was stolen in the Data Breach; (b) the profits MCNA received and is receiving from the use of that information; (c) the amounts that MCNA overcharged Plaintiffs and Class Members for use of MCNA's products and services; and (d) the amounts that MCNA should have spent to provide reasonable and adequate data security to protect Plaintiffs' and Class Members' Private Information.

COUNT V
DECLARATORY JUDGMENT ACT, 28 U.S.C. §§ 2201 *ET SEQ.*

275. Plaintiffs reallege and incorporate by reference the allegations contained in paragraphs 1 through 213 above, as if fully set forth herein.

276. 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 to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal and state statutes described in this Complaint.

277. MCNA owed a duty of care to Plaintiffs and Class Members, which required it to adequately monitor and safeguard Plaintiffs' and Class Members' Private Information.

278. MCNA still possesses the Private Information belonging to Plaintiffs and Class Members.

279. Plaintiffs allege that MCNA's data security measures remain inadequate.

Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their Private Information and the risk remains that further compromises of their Private Information will occur in the future.

280. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. MCNA owes a legal duty to secure Plaintiffs' and Class Members' Private Information under the common law, HIPAA, the FTCA, and other state and federal laws and regulations, as set forth herein;

b. MCNA's existing data monitoring measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect individuals' Private Information; and

c. MCNA continues to breach this legal duty by failing to employ reasonable measures to secure Plaintiffs' and Class Members' Private Information.

281. This Court should also issue corresponding prospective injunctive relief requiring MCNA to employ adequate security protocols consistent with legal and industry standards to protect members' Private Information, including the following:

a. Order MCNA to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

b. Order that, to comply with MCNA's explicit or implicit contractual obligations and duties of care, MCNA must implement and maintain reasonable security and monitoring measures, including, but not limited to:

i. prohibiting MCNA from engaging in the wrongful and unlawful acts

alleged herein;

ii. requiring MCNA to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring MCNA to delete and purge the Private Information of Plaintiffs and Class Members unless MCNA can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring MCNA to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiffs' and Class Members' Private Information;

v. requiring MCNA to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on MCNA's systems on a periodic basis;

vi. prohibiting MCNA from maintaining Plaintiffs' and Class Members' Private Information on a cloud-based database until proper safeguards and processes are implemented;

vii. requiring MCNA to segment data by creating firewalls and access controls so that, if one area of MCNA's network is compromised, hackers cannot gain access to other portions of MCNA's systems;

viii. requiring MCNA to conduct regular database scanning and securing checks;

ix. requiring MCNA to monitor ingress and egress of all network

traffic;

x. requiring MCNA to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling Private Information, as well as protecting the Private Information of Plaintiffs and Class Members;

xi. requiring MCNA to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with MCNA's policies, programs, and systems for protecting personal identifying information;

xii. requiring MCNA to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor MCNA's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated; and

xiii. requiring MCNA to meaningfully educate all Class Members about the threats that it faces because of the loss of its confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

282. If an injunction is not issued, Plaintiffs will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach of MCNA's systems. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

283. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to MCNA if an injunction is issued. The cost of MCNA's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and MCNA has a pre-existing legal duty to employ such measures.

284. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach of MCNA's systems and network, thus preventing future injury to Plaintiffs and other members whose Private Information would be further compromised.

285. Following the issuance of the declaratory relief requested herein, pursuant to 28 U.S.C. § 2202, Plaintiffs and the Class will seek any further necessary or proper relief, including damages, after reasonable notice and hearing, against MCNA.

CLAIM ON BEHALF OF THE ARKANSAS SUBCLASS

COUNT VI
ARKANSAS DECEPTIVE TRADE PRACTICES ACT
A.C.A. §§ 4-88-101 *et seq.*

286. Plaintiff Gannon (for the purposes of this count, "Plaintiff") realleges and incorporates by reference the allegations contained in paragraphs 1 through 213 above, as if fully set forth herein.

287. Plaintiff brings this claim on behalf of herself and the Arkansas Subclass.

288. MCNA is a "person" as defined by A.C.A. § 4-88-102(5).

289. MCNA's products and services are "goods" and "services" as defined by A.C.A. §§ 4-88-102(4) and (7).

290. MCNA advertised, offered, or sold goods or services in Arkansas and engaged in trade or commerce directly or indirectly affecting the people of Arkansas.

291. The Arkansas Deceptive Trade Practices Act ("ADTPA"), A.C.A. §§ 4-88-101 *et seq*., prohibits unfair, deceptive, false, and unconscionable trade practices.

292. MCNA engaged in acts of deception and false pretense in connection with the sale and advertisement of services in violation of A.C.A. § 4-88-108(a)(1) and concealment, suppression, and omission of material facts, with intent that others rely upon the concealment, suppression, or omission in violation of A.C.A. § 4-88-108(a)(2), and engaged in the following deceptive and unconscionable trade practices defined in A.C.A. § 4-88-107:

a. Knowingly making a false representation as to the characteristics, ingredients, uses, benefits, alterations, source, sponsorship, approval, or certification of goods or services or as to whether goods are original or new or of a particular standard, quality, grade, style, or model;

b. Advertising the goods or services with the intent not to sell them as advertised;

c. Knowingly taking advantage of a consumer who is reasonably unable to protect his or her interest; and

d. Engaging in other unconscionable, false, or deceptive acts and practices in business, commerce, or trade.

293. MCNA's unconscionable, false, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Arkansas Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and properly improve security and privacy measures despite knowing the risk of cybersecurity

incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Arkansas Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 45 C.F.R. § 164, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Arkansas Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Arkansas Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 45 C.F.R. § 164;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and Arkansas Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Arkansas Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 45 C.F.R. § 164.

294. MCNA's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of MCNA's data security and ability to protect the confidentiality of consumers' Private Information.

295. MCNA intended to mislead Plaintiff and Arkansas Subclass Members and induce them to rely on its misrepresentations and omissions.

296. Had MCNA disclosed to Plaintiff and Arkansas Subclass Members that its data systems were not secure and, thus, vulnerable to attack, MCNA would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. MCNA was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiff and Arkansas Subclass Members. MCNA accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Arkansas Subclass Members acted reasonably in relying on MCNA's misrepresentations and omissions, the truth of which they could not have discovered.

297. MCNA acted intentionally, knowingly, and maliciously to violate Arkansas' Deceptive Trade Practices Act, and recklessly disregarded Plaintiff's and Arkansas Subclass Members' rights.

298. As a direct and proximate result of MCNA's unconscionable, unfair, and deceptive acts or practices and Plaintiff and Arkansas Subclass Members' reliance thereon, Plaintiff and Arkansas Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as alleged herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial and other accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for MCNA's services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

299. Plaintiff and the Arkansas Subclass Members seek all monetary and non-monetary relief allowed by law, including actual financial losses; injunctive relief; and reasonable attorneys'

fees and costs.

CLAIM ON BEHALF OF THE IOWA SUBCLASS

COUNT VII
IOWA PERSONAL INFORMATION SECURITY BREACH PROTECTION LAW
Iowa Code § 715C.2

300. Plaintiff Carter (for the purposes of this count, "Plaintiff") realleges and incorporates by reference the allegations contained in paragraphs 1 through 213 above, as if fully set forth herein.

301. Plaintiff brings this claim on behalf of himself and the Iowa Subclass.

302. MCNA is a business that owns or licenses computerized data that includes personal information as defined by Iowa Code § 715C.2(1).

303. Plaintiff's and Iowa Subclass Members' Private Information includes personal information as covered under Iowa Code § 715C.2(1).

304. MCNA is required to accurately notify Plaintiff and Iowa Subclass Members if it becomes aware of a breach of its data security system "in the most expeditious manner possible and without unreasonable delay." Iowa Code § 715C.2(1).

305. Because MCNA was aware of a breach in its security systems as of March 6, 2023, it had a duty to disclose the Data Breach in a timely and accurate fashion as mandated by Iowa Code § 715C.2(1). MCNA failed to do so, waiting until late May 2023 to publish a data breach notification on its website.

306. Pursuant to Iowa Code § 715C.2(9), a violation of § 715C.2(1) is an unlawful practice under § 714.16(7).

307. As a direct and proximate result of MCNA's violations of Iowa Code § 715C.2(1), Plaintiff and Iowa Subclass Members suffered damages, as described above.

308. Plaintiff and Iowa Subclass Members seek relief under Iowa Code § 714.16(7), including actual damages; injunctive relief; and any other relief that is just and proper.

CLAIM ON BEHALF OF THE LOUISIANA SUBCLASS

COUNT VIII
LOUISIANA DATABASE SECURITY BREACH NOTIFICATION LAW
La. Rev. Stat. §§ 51:3074(A) *et seq.*

309. Plaintiff Diggs and Plaintiff Souza-Shores (for the purposes of this count, "Plaintiffs") reallege and incorporate by reference the allegations contained in paragraphs 1 through 213 above, as if fully set forth herein.

310. Plaintiffs bring this claim on behalf of themselves and the Louisiana Subclass.

311. MCNA is a business that owns or licenses computerized data that includes personal information as defined by La. Rev. Stat. § 51:3074(C).

312. Plaintiffs and Louisiana Subclass Members' Private Information includes personal information as covered under La. Rev. Stat. § 51:3074(C).

313. MCNA is required to accurately notify Plaintiffs and Louisiana Subclass Members if it becomes aware of a breach of its data security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiffs and Louisiana Subclass Members' Private Information, "in the most expedient time possible and without unreasonable delay but not later than sixty days from the discovery of the breach." La. Rev. Stat. § 51:3074(C).

314. Because MCNA was aware of a breach in its security systems as of March 6, 2023, it had a duty to disclose the Data Breach in a timely and accurate fashion as mandated by La. Rev. Stat. § 51:3074(C). MCNA failed to do so, waiting until late May 2023 to publish a data breach notification on its website.

315. As a direct and proximate result of MCNA's violations of La. Rev. Stat. §

51:3074(C), Plaintiffs and Louisiana Subclass Members suffered damages, as described above.

316. Plaintiffs and Louisiana Subclass Members seek relief under La. Rev. Stat. § 51:3075, including actual damages and any other relief that is just and proper.

CLAIM ON BEHALF OF THE MASSACHUSETTS SUBCLASS

COUNT IX
MASSACHUSETTS CONSUMER PROTECTION ACT, Mass. Gen. Laws Ann. Ch. 93A §§ 1 *et seq.*

317. Plaintiff McCraw (for the purposes of this count, "Plaintiff") realleges and incorporates by reference the allegations contained in paragraphs 1 through 213above, as if fully set forth herein.

318. Plaintiff brings this claim on behalf of himself and the Massachusetts Subclass.

319. MCNA, Plaintiff, and Massachusetts Subclass Members are "persons" as meant by Mass. Gen. Laws. Ann. Ch. 93A § 1(a).

320. MCNA operates in "trade or commerce" as meant by Mass. Gen. Laws Ann. Ch. 93A § 1(b).

321. MCNA advertised, offered, or sold goods or services in Massachusetts and engaged in trade or commerce directly or indirectly affecting the people of Massachusetts, as defined by Mass. Gen. Laws Ann. Ch. 93A § 1(b).

322. MCNA engaged in unfair methods of competition and unfair and deceptive acts and practices in the conduct of trade or commerce, in violation of Mass. Gen. Laws Ann. Ch. 93A § 2(a), including:

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

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 45 C.F.R. § 164, and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff's and Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 45 C.F.R. § 164, and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' Private Information, including duties imposed by the

FTC Act, 15 U.S.C. § 45, HIPAA, 45 C.F.R. § 164, and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05.

323. MCNA's acts and practices were "unfair" because they fall within the scope of common law, statutory, and established concepts of unfairness, given that MCNA solely held the true facts about its inadequate security for Private Information, which Plaintiff and the Massachusetts Subclass Members could not independently discover.

324. MCNA intended to mislead Plaintiff and Massachusetts Subclass Members and induce them to rely on its misrepresentations and omissions.

325. Had MCNA disclosed to Plaintiff and Massachusetts Subclass Members that its data systems were not secure and, thus, were vulnerable to attack, MCNA would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. MCNA was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiff and Massachusetts Subclass Members. MCNA accepted the responsibility of protecting the data but kept the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Massachusetts Subclass Members acted reasonably in relying on MCNA's misrepresentations and omissions, the truth of which they could not have discovered.

326. MCNA's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of MCNA's data security and ability to protect the confidentiality of consumers' Private Information.

327. MCNA acted intentionally, knowingly, and maliciously to violate Massachusetts's Consumer Protection Act, and recklessly disregarded Plaintiff and Massachusetts Subclass

Members' rights.

328. As a direct and proximate result of MCNA's unfair and deceptive, Plaintiff and Massachusetts Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial and other accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for MCNA's services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

329. Plaintiff and Massachusetts Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, double or treble damages, injunctive or other equitable relief, and attorneys' fees and costs.

CLAIM ON BEHALF OF THE MISSISSIPPI SUBCLASS

COUNT X
MISSISSIPPI CONSUMER PROTECTION ACT, Miss. Code §§ 75-24-1 *et seq.*

330. Plaintiff Brown (for the purposes of this count, "Plaintiff") realleges and incorporates by reference the allegations contained in paragraphs 1 through 213above, as if fully set forth herein.

331. Plaintiff brings this claim on behalf of herself and the Mississippi Subclass

332. MCNA is a "person," as defined by Miss. Code § 75-24-3(a).

333. MCNA advertised, offered, or sold goods or services in Mississippi and engaged in trade or commerce directly or indirectly affecting the people of Mississippi, as defined by Miss. Code § 75-24-3(b).

334. MCNA engaged in unfair and deceptive trade acts or practices, including:

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

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 45 C.F.R. § 164, and Miss. Code. Ann. § 75-24-29, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff's and Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 45 C.F.R. § 164, and Miss. Code. Ann. § 75-24-29;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of

Plaintiff's and Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 45 C.F.R. § 164, and Miss. Code. Ann. § 75-24-29.

335. The above-described conduct violated Miss. Code Ann. § 75-24-5(2), including:

a. Representing that goods or services have approval, characteristics, uses, or benefits that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another; and

c. Advertising goods or services with intent not to sell them as advertised.

336. MCNA intended to mislead Plaintiff and Mississippi Subclass Members and induce them to rely on its misrepresentations and omissions.

337. MCNA's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of MCNA's data security and ability to protect the confidentiality of consumers' Private Information.

338. Had MCNA disclosed to Plaintiff and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, MCNA would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. MCNA was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiff and the Subclass. MCNA accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on MCNA's misrepresentations and omissions, the truth of which they could not have discovered.

339. MCNA had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extensivity of the Private Information in its possession, and the

generally accepted professional standards. Such a duty is implied by law due to the nature of the relationship between consumers-including Plaintiff and the Mississippi Subclass and MCNA. MCNA's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

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

340. MCNA acted intentionally, knowingly, and maliciously to violate Mississippi's Consumer Protection Act, and recklessly disregarded Plaintiff and Mississippi Subclass Members' rights. MCNA's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

341. As a direct and proximate result of MCNA's unfair and deceptive acts or practices and Plaintiff's and Mississippi Subclass Members' purchase of goods or services primarily for personal, family, or household purposes, Plaintiff and Mississippi Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial and other accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for MCNA's services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

342. MCNA's violations present a continuing risk to Plaintiff and Mississippi Subclass

Members as well as to the general public.

343. Plaintiff and Mississippi Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, restitution and other relief under Miss. Code § 75-24-11, injunctive relief, punitive damages, and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE NEBRASKA SUBCLASS

COUNT XI
NEBRASKA CONSUMER PROTECTION ACT
Neb. Rev. Stat. §§ 59-1601 *et seq*.

344. Plaintiff Shaffer (for the purposes of this count, "Plaintiff") realleges and incorporates by reference the allegations contained in paragraphs 1 through 213above, as if fully set forth herein.

345. Plaintiff brings this claim on behalf of herself and the Nebraska Subclass.

346. MCNA is a person engaged in trade or commerce as contemplated by the Nebraska Consumer Protection Act, Neb. Rev. Stat. §§ 59-1601 *et seq.* ("NCPA").

347. MCNA participated in unfair and deceptive acts and practices that violated NCPA, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Nebraska Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Nebraska Subclass Members' Private Information,

including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA, 45 C.F.R. § 164, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Nebraska Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Nebraska Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA, 45 C.F.R. § 164;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and Nebraska Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Nebraska Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA, 45 C.F.R. § 164.

348. MCNA's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of MCNA's data security and ability to protect the confidentiality of consumers' Private Information.

349. MCNA intended to mislead Plaintiff and Nebraska Subclass Members and induce them to rely on its misrepresentations and omissions.

350. MCNA's conduct was not only deceptive, but also unfair within the meaning of NCPA because it constitutes immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or

competition. The injuries suffered by Plaintiff and the Nebraska Subclass are not outweighed by any countervailing benefits to consumers or competition. Because MCNA is solely responsible for securing its networks and protecting Private Information, there is no way Plaintiff and Nebraska Subclass Members could have known about MCNA's inadequate data security practices or avoided the injuries they sustained. There were reasonably available alternatives to further MCNA's legitimate business interests, other than its conduct responsible for the Data Breach.

351. As a direct and proximate result of MCNA's unfair, and deceptive acts and practices, Plaintiff and Nebraska Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as alleged herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial and other accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for MCNA's services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

352. Plaintiff and Nebraska Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages; injunctive relief under Neb. Rev. Stat. § 59-1609; the costs of this action including reasonable attorneys' fees; and any other relief that is just and proper.

COUNT XII
NEBRASKA UNIFORM DECEPTIVE TRADE PRACTICES ACT
Neb. Rev. Stat. §§ 87-301 *et seq.*

353. Plaintiff Shaffer (for the purposes of this count, "Plaintiff") realleges and incorporates by reference the allegations contained in paragraphs 1 through 213above, as if fully set forth herein.

354. Plaintiff brings this claim on behalf of herself and the Nebraska Subclass.

355. Plaintiff, Nebraska Subclass Members, and MCNA all qualify as persons engaged in trade or commerce as contemplated by the Nebraska Uniform Deceptive Trade Practices Act, Neb. Rev. Stat. § 87-301 *et seq.* ("NUDTPA").

356. MCNA's implied and express representations that it would adequately safeguard Plaintiff's and Nebraska Subclass Members' Private Information are representations as to characteristics, uses, or benefits of services that such services did not actually have, in violation of Neb. Rev. Stat. § 87-302(a)(5).

357. MCNA's implied and express representations that it would adequately safeguard Plaintiff's and Nebraska Subclass Members' Private Information are representations as to the particular standard, quality, or grade of services that such services did not actually have (as the data security services were of another, inferior quality), in violation of Neb. Rev. Stat. § 87-302(a)(8).

358. MCNA knowingly made false or misleading statements in its Notice of Privacy Practices regarding the use of personal information submitted by Customers, in that it did not "safeguard[] [its] members' protected health information" and protect "individually identifiable information, like your name, address, telephone number, [and] Social Security number"[59] in violation of Neb. Rev. Stat. § 87-302(a)(15).

359. These violations have caused financial injury to Plaintiff and Nebraska Subclass Members.

360. Accordingly, Plaintiff and Nebraska Subclass Members seek injunctive relief under NUDTPA; the costs of this action including reasonable attorneys' fees; and any other relief that is

[59] *Our Privacy Practices*, MCNA, https://www.mcna.net/en/privacy (last visited Nov. 11, 2023).

just and proper.

CLAIMS ON BEHALF OF THE NEW YORK SUBCLASS

COUNT XIII
NEW YORK GENERAL BUSINESS LAW, N.Y. Gen. Bus. Law §§ 349 *et seq.*

361. Plaintiff Kachakech (for the purposes of this count, "Plaintiff") realleges and incorporates by reference the allegations contained in paragraphs 1 through 213 above, as if fully set forth herein.

362. Plaintiff brings this claim on behalf of himself and the New York Subclass.

363. MCNA Dental and Healthplex engaged in deceptive acts or practices in the conduct of their business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

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

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 45 C.F.R. § 164, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff's and Subclass Members' Private Information, including by implementing and

maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 45 C.F.R. § 164;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 45 C.F.R. § 164.

364. MCNA Dental and Healthplex's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of MCNA Dental and Healthplex's data security and ability to protect the confidentiality of consumers' Private Information.

365. MCNA Dental and Healthplex acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiff and New York Subclass Members' rights.

366. As a direct and proximate result of MCNA Dental and Healthplex's deceptive and unlawful acts and practices, Plaintiff and New York Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time

and expenses related to monitoring their financial and other accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for Healthplex's services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

367. MCNA Dental and Healthplex's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the New Yorkers affected by the Data Breach.

368. The above deceptive and unlawful practices and acts by MCNA Dental and Healthplex caused substantial injury to Plaintiff and New York Subclass Members that they could not reasonably avoid.

369. Plaintiff and New York Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs.

CLAIM ON BEHALF OF THE TEXAS SUBCLASS

COUNT XIV
TEXAS DECEPTIVE TRADE PRACTICES–CONSUMER PROTECTION ACT
Texas Bus. & Com. Code §§ 17.41 *et seq.*

370. Plaintiff Acosta and Plaintiff Hughes (for the purposes of this count, "Plaintiffs") reallege and incorporate by reference the allegations contained in paragraphs 1 through 213 above, as if fully set forth herein.

371. Plaintiffs bring this claim on behalf of themselves and the Texas Subclass.

372. MCNA is a "person," as defined by the Texas Trade Practices–Consumer Protection Act ("DTPA"), Tex. Bus. & Com. Code § 17.45(3).

373. Plaintiffs and the Texas Subclass Members are "consumers," as defined by Tex.

Bus. & Com. Code § 17.45(4).

374. MCNA advertised, offered, or sold goods or services in Texas and engaged in trade or commerce directly or indirectly affecting the people of Texas, as defined by Tex. Bus. & Com. Code § 17.45(6).

375. MCNA engaged in false, misleading, or deceptive acts and practices, in violation of Tex. Bus. & Com. Code § 17.46(b), including:

a. Representing that goods or services have approval, characteristics, uses, or benefits that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade, if they are of another; and

c. Advertising goods or services with intent not to sell them as advertised;

d. Failing to disclose information concerning goods or services which was known at the time of the transaction if such failure to disclose such information was intended to induce the consumer into a transaction into which the consumer would not have entered had the information been disclosed.

376. MCNA's false, misleading, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Texas Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the

security and privacy of Plaintiffs' and Texas Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; HIPAA, 45 C.F.R. § 164; and Texas' data security statute, Tex. Bus. & Com. Code § 521.052, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Texas Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Texas Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; HIPAA, 45 C.F.R. § 164; and Texas' data security statute, Tex. Bus. & Com. Code § 521.052;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiffs' and Texas Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Texas Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; HIPAA, 45 C.F.R. § 164; and Texas' data security statute, Tex. Bus. & Com. Code § 521.052.

377. MCNA intended to mislead Plaintiffs and Texas Subclass Members and induce them to rely on its misrepresentations and omissions.

378. MCNA's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of MCNA's data security and ability to protect the confidentiality of consumers' Private Information.

379. Had MCNA disclosed to Plaintiffs and Texas Subclass Members that its data systems were not secure and, thus, vulnerable to attack, MCNA would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. MCNA was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs and Texas Subclass Members. MCNA accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiffs and Texas Subclass Members acted reasonably in relying on MCNA's misrepresentations and omissions, the truth of which they could not have discovered.

380. MCNA had a duty to disclose the above facts due to the circumstances of this case, the sensitivity and extent of the Private Information in its possession, and the generally accepted professional standards. Such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiffs and Texas Subclass Members, and MCNA because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in MCNA. MCNA's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, while purposefully withholding material facts from Plaintiffs and Texas Subclass Members that contradicted these representations.

381. MCNA engaged in unconscionable actions or courses of conduct, in violation of Tex. Bus. & Com. Code Ann. § 17.50(a)(3). MCNA engaged in acts or practices which, to

consumers' detriment, took advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree.

382. Consumers, including Plaintiffs and Texas Subclass Members, lacked knowledge about deficiencies in MCNA's data security because this information was known exclusively by MCNA. Consumers also lacked the ability, experience, or capacity to secure the Private Information in MCNA's possession or to fully protect their interests with regard to their data. Plaintiffs and Texas Subclass Members lack expertise in information security matters and do not have access to MCNA's systems in order to evaluate its security controls. MCNA took advantage of its special skill and access to Private Information to hide its inability to protect the security and confidentiality of Plaintiffs' and Texas Subclass Members' Private Information.

383. MCNA intended to take advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree, with reckless disregard of the unfairness that would result. The unfairness resulting from MCNA's conduct is glaringly noticeable, flagrant, complete, and unmitigated. The Data Breach, which resulted from MCNA's unconscionable business acts and practices, exposed Plaintiffs and Texas Subclass Members to a wholly unwarranted risk to the safety of their Private Information and the security of their identity or credit, and worked a substantial hardship on a significant and unprecedented number of consumers. Plaintiffs and Texas Subclass Members cannot mitigate this unfairness because they cannot undo the Data Breach.

384. MCNA acted intentionally, knowingly, and maliciously to violate Texas' Deceptive Trade Practices–Consumer Protection Act, and recklessly disregarded Plaintiffs' and Texas Subclass Members' rights.

385. As a direct and proximate result of MCNA's unconscionable and deceptive acts or

practices, Plaintiffs and Texas Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, non-monetary damages, as alleged herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial and other accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for MCNA's services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach. MCNA's unconscionable and deceptive acts or practices were a producing cause of Plaintiffs' and Texas Subclass Members' injuries, ascertainable losses, economic damages, and non- economic damages, including their mental anguish.

386. MCNA's violations present a continuing risk to Plaintiffs and Texas Subclass Members, as well as to the general public.

387. On November 13, 2023, counsel for Plaintiffs provided written notice via certified mail to MCNA of the intent to pursue claims under the DTPA and an opportunity for MCNA to cure. Plaintiffs' written notice set forth the violations of MCNA's duty to implement and maintain reasonable security procedures and practices alleged in this Complaint.

388. Contemporaneous with the filing of this Complaint, pursuant to Tex. Bus. & Com. Code Ann. § 17.501, Plaintiffs' counsel will send to the Consumer Protection Division a copy of the written notice sent to MCNA.

389. Plaintiffs and Texas Subclass Members seek damages, including economic damages, damages for mental anguish, statutory damages in the amount of three times the economic and mental anguish damages, as MCNA's acts were committed intentionally or knowingly, injunctive relief, other equitable relief the Court deems proper, costs, and reasonable and necessary attorneys' fees.

CLAIM ON BEHALF OF THE UTAH SUBCLASS

COUNT XV
UTAH CONSUMER SALES PRACTICES ACT
Utah Code §§ 13-11-1 *et seq.*

390. Plaintiff Hathaway (for the purposes of this count, "Plaintiff") realleges and incorporates by reference the allegations contained in paragraphs 1 through 213 above, as if fully set forth herein.

391. Plaintiff brings this claim on behalf of herself and the Utah Subclass.

392. MCNA is a "person" as defined by Utah Code § 13-11-3(5).

393. MCNA is a "supplier" as defined by Utah Code § 13-11-3(6) because it regularly solicits, engages in, or enforces consumer transactions, whether or not it deals directly with the consumer.

394. MCNA engaged in deceptive and unconscionable acts and practices in connection with consumer transactions, in violation of Utah Code §§ 13-11-4 and 13-11-5, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Utah Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Utah Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; HIPAA, 45 C.F.R. § 164; and the Utah Protection of Personal Information Act, Utah Code § 13-44-201, which was a

direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Utah Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Utah Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; HIPAA, 45 C.F.R. § 164; and the Utah Protection of Personal Information Act, Utah Code § 13-44-201;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and Utah Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Utah Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; HIPAA, 45 C.F.R. § 164; and the Utah Protection of Personal Information Act, Utah Code § 13-44-201.

395. MCNA's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of MCNA's data security and ability to protect the confidentiality of consumers' personal financial information.

396. MCNA intended to mislead Plaintiff and Utah Subclass Members and induce them to rely on its misrepresentations and omissions.

397. MCNA's conduct was not only deceptive, but also unfair within the meaning of because it constitutes immoral, unethical, oppressive, and unscrupulous activity, caused substantial

injury to consumers and businesses, and provided no benefit to consumers or competition. The injuries suffered by Plaintiff and the Utah Subclass are not outweighed by any countervailing benefits to consumers or competition. Because MCNA is solely responsible for securing its networks and protecting Private Information, there is no way Plaintiff and Utah Subclass Members could have known about MCNA's inadequate data security practices or avoided the injuries they sustained. There were reasonably available alternatives to further MCNA's legitimate business interests, other than its conduct responsible for the Data Breach.

398. As a direct and proximate result of MCNA's unfair, and deceptive acts and practices, Plaintiff and Utah Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as alleged herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial and other accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for MCNA's services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

399. Plaintiff and Utah Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages; statutory damages of $2,000 per violation; amounts necessary to avoid unjust enrichment under Utah Code §§ 13-11-19 *et seq.*; injunctive relief; reasonable attorneys' fees and costs; and any other relief that is just and proper.

PRAYER FOR RELIEF

WHEREFORE Plaintiffs, individually and on behalf of all others similarly situated, request the following relief:

A. An order certifying this action as a class action and appointing Plaintiffs as Class

representatives and the undersigned as Class Counsel;

B. A declaration that MCNA breached its duties to Plaintiffs and Class Members;

C. A mandatory injunction directing MCNA to adequately safeguard the Private Information of Plaintiffs and the Class hereinafter by implementing improved security procedures and measures;

D. A mandatory injunction requiring that MCNA provide notice to each Class Member relating to the full nature and extent of the Data Breach and the disclosure of Private Information to unauthorized persons;

E. An order enjoining MCNA from further unfair, deceptive, and unconscionable practices and making untrue statements about the Data Breach and the stolen Private Information;

F. An award of damages, including actual, nominal, consequential damages, statutory, and/or punitive, as allowed by law in an amount to be determined;

G. An award of pre- and post-judgment interest, costs, attorneys' fees, expenses, and interest as permitted by law;

H. For all other orders, findings, and determinations identified and sought in this Complaint; and

I. Such other and further relief as this court may deem just and proper.

I. JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury for all issues so triable as of right.

Dated: January 30, 2024.

Respectfully Submitted,

By: *Stephanie A. Casey*
Stephanie A. Casey FBN 97483
COLSON HICKS EIDSON, P.A.
255 Alhambra Circle, Penthouse

Coral Gables, Florida 33134
Telephone: (305) 476-7400
scasey@colson.com

Liaison Counsel for Plaintiffs and the Putative Classes

Jeff Ostrow FBN 121452
KOPELOWITZ OSTROW FERGUSON WEISELBERG GILBERT
One West Las Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Telephone: (954) 332-4200
ostrow@kolawyers.com

Peter Prieto FBN 501492
PODHURST ORSECK, P.A.
One S.E. 3rd Avenue, Suite 2300
Miami, Florida 33131
Telephone: (305) 358-2800
pprieto@podhurst.com

Interim Co-Lead Counsel for Plaintiffs and the Putative Classes

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing has been served via email via the CM/ECF system on all counsel of record on this 30th day of January, 2024.

Unless there is an agreement to waive service, MCNA Insurance Company and Healthplex, Inc. will be formally served through their registered agents.

/s/ Stephanie A. Casey
Stephanie A. Casey

EXHIBIT A

mcnadental

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

To Enroll, Please Call:
1-888-220-5006
Or Visit:
https://response.idx.us/MCNA-Information
Enrollment Code: 7SAG5ZT86W

40065226008207540
000 0008573 00000000 0001 0004 02144 INS: 0 0

ALICIAH K SOUZA
10714 RITCHIE ST
BASTROP LA 71220-1869

54
14644

May 26, 2023

Su información personal puede haber estado involucrada en un incidente de datos. Si desea recibir una version de esta carta en español, por favor llame 1-888-220-5006.

Notice of Data Breach

Dear Aliciah K Souza:

We are sorry to tell you about a privacy event. This letter is from MCNA. We work with the Louisiana Department of Health; and the Children's Health Insurance Program to help provide benefits. This event may have involved your information.

What happened?
On March 6, 2023, MCNA became aware of certain activity in our computer system that happened without our permission. We quickly took steps to stop that activity. We began an investigation right away. A special team was hired to help us. We learned a cybercriminal was able to see and take copies of some information in our computer system between February 26, 2023 and March 7, 2023.

What information may have been involved?
On May 4, 2023, we told the state Medicaid agency that this event may have involved your information. Here is the kind of information that was seen and taken:

- Information used to contact you, like first and last name, address, date of birth, phone number, email
- Social Security number
- Driver's license number/other government-issued ID number
- Health insurance (plan information, insurance company, member number, Medicaid-Medicare ID numbers)
- Care for teeth or braces (visits, dentist name, doctor name, past care, x-rays/photos, medicines, and treatment)
- Bills and insurance claims

Some of this information was for a parent, guardian, or guarantor. A guarantor is the person who paid the bill. Information which was seen and taken was not the same for everyone.

Why did this happen?
A cybercriminal accessed our computer system without our permission.

What was done about it?
When we learned about the activity, we immediately began an investigation. Law enforcement was contacted. We are also making our computer systems even stronger than before because we do not want this to happen again.

We would like to offer you a free identity theft protection service. We will pay for the cost of this service for 1 year so that it is free for you. We have attached steps on how to sign up for this free service.

For Residents of Maryland

You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, http://www.marylandattorneygeneral.gov/.

For Residents of Massachusetts

You have the right to obtain a police report with respect to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For Residents of New Mexico

New Mexico consumers have the right to obtain a security freeze or submit a declaration of removal.

You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

(1) the unique personal identification number, password or similar device provided by the consumer reporting agency;

(2) proper identification to verify your identity; and

(3) information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

For Residents of New York

You may also obtain information about security breach response and identity theft prevention and protection from the New York Attorney General's Office:

Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, www.ag.ny.gov.

EXHIBIT B

mcnadental healthplex

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

To Enroll, Please Call:
1-888-220-5006
Or Visit:
https://response.idx.us/MCNA-Information
Enrollment Code: 9KERWWC3MS

40065226008564489
000 0007117 00000000 0001 0004 01780 INS: 0 0

TAREK KACHAKECH
[redacted]
NEW YORK NY [redacted]
20
4280

May 26, 2023

Su información personal puede haber estado involucrada en un incidente de datos. Si desea recibir una version de esta carta en español, por favor llame 1-888-220-5006.

Notice of Data Breach

Dear Tarek Kachakech:

We are sorry to tell you about a privacy event. This letter is from MCNA Dental Plan. We worked with Healthplex, Inc. to help provide dental benefits under your insurance plan from Metroplus Health Plan, Inc.. This event may have involved your information.

What happened?
On March 6, 2023, MCNA became aware of certain activity in our computer system that happened without our permission. We quickly took steps to stop that activity. We began an investigation right away. A special team was hired to help us. We learned a criminal was able to see and take copies of some information in our computer system between February 26, 2023 and March 7, 2023. MCNA notified Healthplex on March 29, 2023.

What information may have been involved?
Between May 10, 2023 and May 23, 2023, Healthplex told your insurance plan that this event may have involved your information. Here is the kind of information that may have been seen and taken:

- Information used to contact you, like first and last name, address, date of birth, phone number, email
- Social Security number
- Driver's license number/other government-issued ID number
- Health insurance (plan information, insurance company, member number, Medicaid-Medicare ID numbers)
- Care for teeth or braces (visits, dentist name, doctor name, past care, x-rays/photos, medicines, and treatment)
- Bills and insurance claims

Some of this information was for a parent, guardian, or guarantor. A guarantor is the person who paid the bill. Information which was seen and taken was not the same for everyone.

Why did this happen?
A criminal accessed our computer system without our permission.

What was done about it?
When we learned about the activity, we immediately began an investigation. Law enforcement was contacted. We are also making our computer systems even stronger than before because we do not want this to happen again.

We would like to offer you an identity theft protection service. We will pay for the cost of this service for 1 year so that it is free for you. We have attached steps on how to sign up for this service.

What should I do?
You can sign up for the identity theft protection service. Please check your bills and accounts to be sure they look correct. We have attached steps on how to do that.