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.

SECOND 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, Inc."), MCNA Insurance Company d/b/a MCNA Dental ("MCNAIC") (collectively, "MCNA") and Healthplex, Inc. ("Healthplex") (all collectively, "Defendants"). 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 Defendants' failure to secure the highly sensitive personal identifiable information ("PII") and protected health information ("PHI") (collectively "Private

Information") of Plaintiffs and the members of the proposed Class (defined *infra* ¶ 208) for whom Defendants 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. Healthplex is a wholly-owned subsidiary of MCNA, Inc. or one of its affiliated entities, and provides insurance in New York. In these roles, for years, Defendants 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, Defendants 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 Defendants' 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 ("Data Breach").[2]

[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 Sept. 4, 2024).

4. Defendants' investigation concluded the Private Information compromised in the 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 Defendants' 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, Defendants did not pay any amount to resolve the ransomware demand. Consequently, 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 Defendants' 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. Defendants compounded this harm by waiting more than two months before notifying affected Customers their highly sensitive Private Information was now in the hands of sophisticated cybercriminals.

7. It was not until May 26, 2023—eleven weeks after Defendants detected the attack on March 6, 2023—that Defendants began notifying Customers of the Data Breach. Defendants'

---

[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 (last visited Nov. 11, 2023)).
[4] *Id.*
[5] *Id.*
[6] *Id.*

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 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 Defendants' deficient cybersecurity practices, and the wealth of information and warnings available to Defendants 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, Defendants were required by law to exercise reasonable care and comply with industry and statutory requirements to protect that information—and they 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 including Defendants 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, Defendants disregarded the rights of Plaintiffs and Class Members by 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. Defendants' woefully inadequate data security measures made the Data Breach

a foreseeable, and even likely, consequence of its negligence.

12. Defendants admit Social Security numbers, driver's licenses, and other government ID data was taken in the Data Breach. These types 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 PII used to provide proof of identity for all manner 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 methods, criminals can assemble a full dossier of Private Information on an individual 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 is aware the PII was stolen.[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 PHI's high value, the FBI has long warned healthcare providers they are likely to be the targets of cyberattacks like the attack that caused the Data Breach.[10]

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

18. Furthermore, 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 who do not pay and as a means to

---

[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.

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) lower credit scores; (l) lost work time; (m) anxiety, annoyance, and nuisance; and (n) continued risk to their Private Information, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail 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 Defendants had they known Defendants 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 Defendants responsible for the injuries it inflicted on Plaintiffs and approximately 8.9 million similarly situated people due to their 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 Defendants.

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 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 MCNA, 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 MCNA, 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 received benefits from MCNA by virtue of his health plan membership.

27. Plaintiff Acosta received a Notice Letter from "MCNA Dental" dated May 26, 2023, disclosing 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 received benefits from MCNA by virtue of her health plan membership.

33. Plaintiff Brown received a Notice Letter from "MCNA Dental" 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 received benefits from MCNA by virtue of his health plan membership.

39. Plaintiff Carter received a Notice Letter from "MCNA Dental" 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 60-65 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 received benefits from MCNA by virtue of her health plan membership.

45. Plaintiff Crowe received a Notice Letter from "MCNA Dental" 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 received benefits from MCNA by virtue of her medical plan membership.

51. Plaintiff Diggs received a Notice Letter from "MCNA Dental" 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 received benefits from MCNA by virtue of her health plan membership.

57. Plaintiff Gannon received a Notice Letter from "MCNA Dental" 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 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 received benefits from MCNA by virtue of his health plan membership.

63. Plaintiff Hanekom received a Notice Letter from "MCNA Dental" 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 regularly 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 received benefits from MCNA by virtue of her health plan membership.

69. Plaintiff Hathaway received a Notice Letter from "MCNA Dental" 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 received benefits from MCNA by virtue of her health plan membership.

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

76. Since the Data Breach, Plaintiff Hughes had to freeze her debit card 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 received 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. *See* Ex. B.

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 received benefits from MCNA by virtue of his health plan membership.

87. Plaintiff McCraw received a Notice Letter from "MCNA Dental" 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 credit card to make a purchase in the amount of $12.48 on Walmart.com. As a result, the credit card company 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 14-16 hours reviewing his financial accounts for identity theft and fraud, researching the Data Breach, reviewing his credit report, and communicating with his credit card company 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, and has to spend time unfreezing it any time he wants to apply for a loan or other form of credit. 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 Dental" 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 medical provider 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 received benefits from MCNA by virtue of her health membership.

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

100. Since the Data Breach, Plaintiff Souza-Shores has had to close her debit card and open a new one after unauthorized charges appeared on it three successive times, 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 received benefits from MCNA by virtue of her health plan membership.

105. Plaintiff Spears received a Notice Letter from "MCNA Dental" 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 received benefits from MCNA by virtue of her health plan membership.

111. Plaintiff Winkler received a Notice Letter from "MCNA Dental" 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 received benefits from MCNA by virtue of her health plan membership.

117. Plaintiff Zurline received a Notice Letter from "MCNA Dental" 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. MCNA, 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 MCNA, Inc. or one of its affiliated entities.

FACTUAL ALLEGATIONS

A. Defendants Collect and Use 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's website states that "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."[13]

125. Specifically, MCNA, Inc. operates as a dental insurer in Florida (through Florida Health Kids Corporation for CHIP insureds, and through the Florida Agency for Health Care Administration for Medicaid insureds), and outside Florida, it operates as a third-party administrator providing operational services such as claims processing.

126. MCNAIC operates or operated as a dental insurer in Arkansas, Idaho, Iowa, Louisiana, Nebraska, Texas, and Utah.

127. Healthplex operates as a dental insurer in the state of New York, including for government-sponsored plans. In 2019, Healthplex was acquired by MCNA, Inc. or one of its affiliated entities.[14]

128. Defendants collect 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 Defendants directly, but through Medicaid, CHIP, or Medicare. This personal data is collectively managed and maintained on MCNA computer systems for both MCNA entities and Healthplex whose data was part of the Data Breach.

---

[11] *Company Overview*, MCNA, https://www.mcna.net/en/company-overview (last visited Jan. 20, 2024).
[12] *Id*.
[13] *Home*, MCNA, https://www.mcna.net/en/home (last visited Nov. 11, 2023).
[14] *See, e.g.*, https://www.prnewswire.com/news-releases/healthplex-acquired-by-affiliates-of-mcna-dental-300920114.html (last visited Jan. 20, 2024).

129. MCNA'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. . . . "[15] MCNA also claims it is "committed to complying with the requirements and standards of the Health Insurance Portability and Accountability Act of 1996 (HIPAA)."[16] 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."[17]

130. MCNA states it must follow the privacy practices in its Notice of Privacy Practices, which applied to both MCNA, Inc. and MCNAIC.[18]

131. MCNA 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."[19]

132. MCNA acknowledges "[t]he law says MCNA has to keep your health information private."[20] 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."[21]

133. MCNA 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."[22] The Notice of Privacy

[15] *Our Privacy Practices*, MCNA, https://www.mcna.net/en/privacy (last visited Jan. 20, 2024).
[16] *Id.*
[17] *Id.*
[18] *Id.*
[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] *Id.*

Practices lists several ways MCNA may use its Customers' information, including, *inter alia*, for research, to comply with the law, and to address workers' compensation claims.[23]

134. MCNA promises to "let you know promptly if a breach occurs that may have compromised the privacy or security of your information."[24] 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.

135. MCNA'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."[25] MCNA's website also states "DentalTrac™ is hosted across multiple geographically dispersed, military grade, secure, and state-of-the-art data centers" and 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."[26]

136. Healthplex's Notice of Privacy Practices states: "We are required by law to maintain the privacy and security of your protected health information."[27] 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,

---

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

and is collected from the individual or is obtained in connection with providing health care coverage to the individual."[28]

137. Plaintiffs and Class Members relied on Defendants' promises to keep their Private Information confidential and securely maintained, and to only make authorized disclosures of this information. Defendants failed to do so.

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

138. According to the Notice of Data Breach posted on MCNA's website, Defendants "became aware that an unauthorized party was able to access certain MCNA systems" on March 6, 2023, and "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."[29]

139. In other words, Defendants' 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.

140. At all relevant times, Defendants were aware, or reasonably should have been aware, that the Private Information they collected, maintained, and stored in their 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.

---

[28] Financial Information Privacy Notice, HEALTHPLEX, available at https://www.healthplex.com/doc/no/F-2507ND (last visited Jan. 20. 2024).

[29] *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").

141. 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.

142. Defendants were fully aware the healthcare benefits industry is a prime target for cyber threats.[30] 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%, making it the fifth most common industry targeted by cyberattacks.[31]

143. 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 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.

---

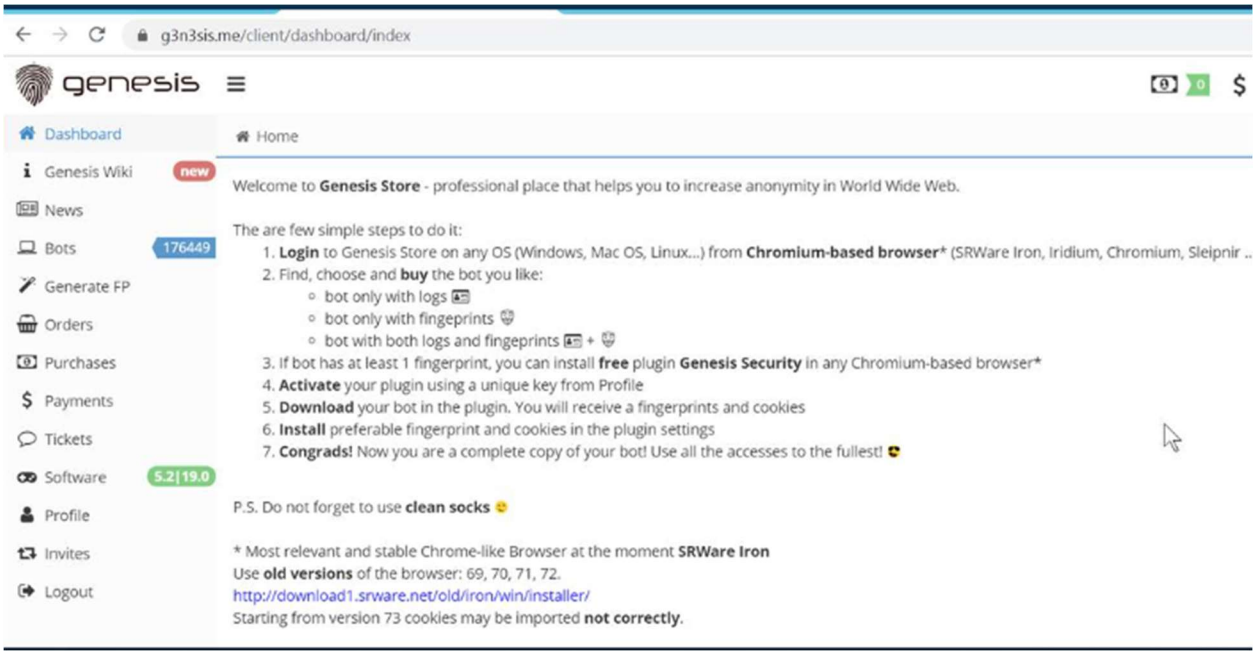
[30] *See* Finkle, *FBI warns healthcare firms they are targeted by hackers*, *supra* n.10.
[31] Check Point Research Team, *Check Point Research: Cyber Attacks Increased 50% Year over Year*, Check Point (Jan. 10, 2022), https://blog.checkpoint.com/security/check-point-research-cyber-attacks-increased-50-year-over-year.
[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.
[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).

144. Defendants knew or should have known of the tactics that groups like LockBit employ, and how to guard against them. For one thing, MCNA is a member of Healthcare Information and Management Systems Society (HIMSS), a nonprofit that advises on the best use of information technology and management systems.[35]

145. Moreover, Defendants knew or should have known of ransomware targeting their systems available on the dark web. MCNA is a longstanding member of the Health-Information Sharing and Analysis Center ("Health-ISAC"), a nonprofit that proactively alerts its members of cybersecurity threats,[36] All Health-ISAC subscribers receive for free Level 1 and Level 2 alerts, and members like MCNA receive Level 3 alerts, including from the FBI. Therefore, the cost to Defendants of taking the precaution of monitoring relevant cybersecurity alerts would have been negligible.

146. Prior to the Data Breach, Defendants had many chances to increase their cybersecurity measures. For example, since as early as 2019, Genesis Market, dark web marketplace for popular and considered highly reputable among cybercriminals, advertised credentials for mcna.net. For illustration, this is a screenshot of the well-known Genesis Market:

[35] https://www.himss.org/ (last visited Sept. 10, 2024).
[36] https://h-isac.org/ (last visited Sept. 10, 2024).



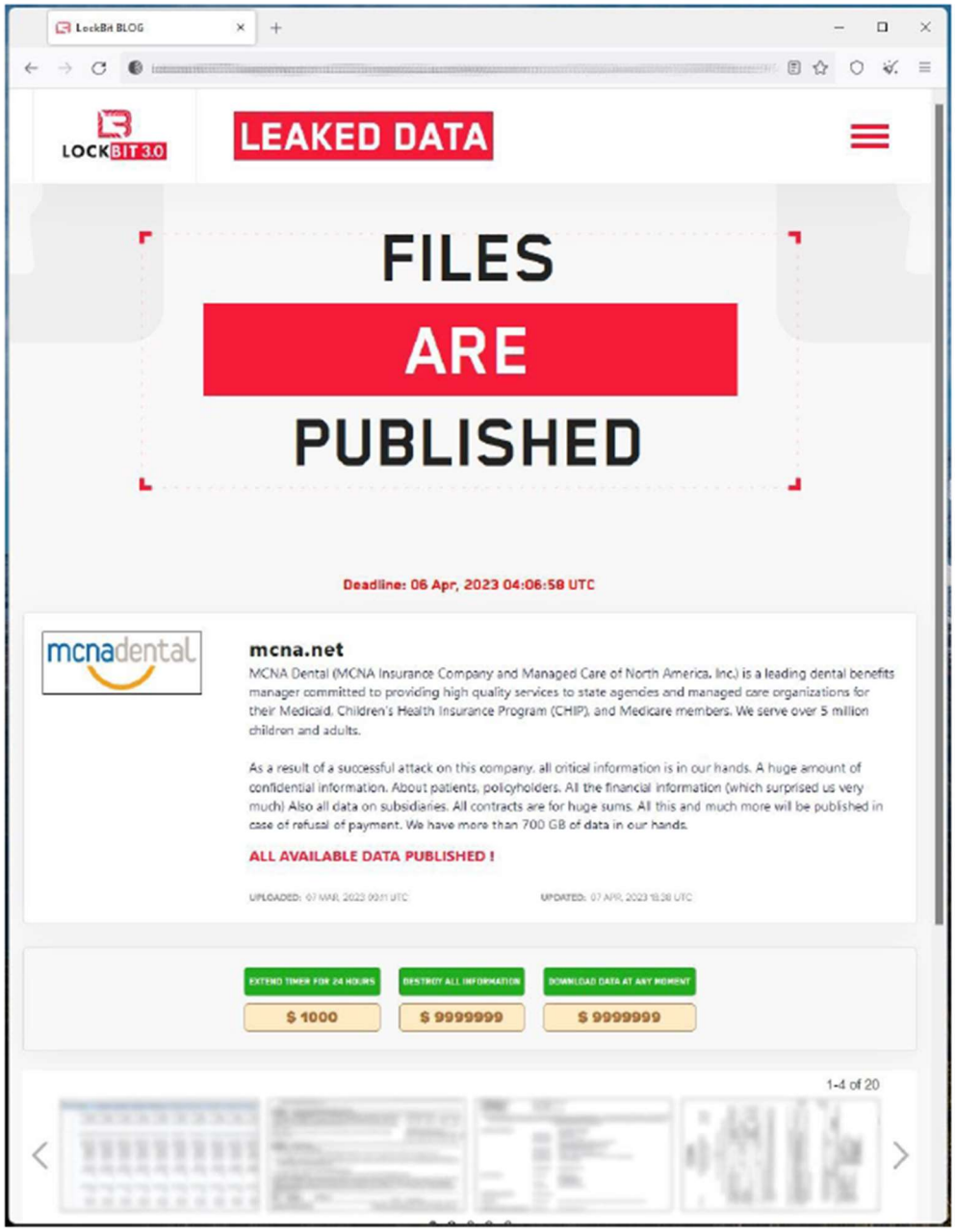
Then, since as early as August 28, 2021, The Russianmarket, another dark web marketplace, was advertising ransomware tools to access the MCNA patient portal. In addition, between September 3, 2021, and October 25, 2022, 2Easy, a dark web marketplace known for selling ransomware tools to access vulnerable websites,[37] was advertising the sale of ransomware to access the MCNA patient portal on the dark web, and offered a full refund if the product did not work.

147. These vulnerabilities may have directly contributed to the Data Breach. At the very least, these vulnerabilities should have been warning signs to Defendants to increase their general data security.

148. With the Private Information secured and stolen by LockBit, the hackers then purportedly issued a ransom demand to Defendants of $10 million. On information and belief, Defendants 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

[37] Bill Toulas, *2easy now a significant dark web marketplace for stolen data*, BLEEPING COMPUTER, https://www.bleepingcomputer.com/news/security/2easy-now-a-significant-dark-web-marketplace-for-stolen-data/ (last visited Sept. 1, 2024).

from the Data Breach on its dump site:



149. 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. 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 harm to Plaintiffs and Class Members.

150. LockBit's history[38] makes the disclosure of Plaintiffs' and Class Members' Private Information to illegal operators a near certainty.[39]

151. Further, the proof data openly published by LockBit proves it has taken far more information from Defendants than they admits in the Notice Letters. LockBit claims (with evidence) that it exfiltrated over 700 GB of data from Defendants, which appears to be most—if not all—of the document data Defendants hold. The proof exhibited by LockBit includes documents regarding employees and Plaintiffs, as well as Defendants' 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 (a) Defendants do not know the extent of information taken and (b) the theft includes *all* information Defendants hold regarding Plaintiffs.

C. Defendants Failed to Comply with Regulatory Requirements and Industry Practices.

152. Federal and state regulators have established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and the healthcare sector. There are a number of state and federal laws, requirements, and industry standards governing the protection of Private Information.

153. For example, at least 24 states have enacted laws addressing data security practices

[38] 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).

[39] "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).

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 Defendants "take reasonable measures to protect and secure data in electronic form containing personal information." Fla. Stat. § 501.171(2).

154. 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.[40]

155. 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.[41]

156. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[42] The guidelines note businesses should protect the personal customer information they keep; properly dispose of Private Information no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and

---

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

[41] *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).

[42] *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).

implement policies to correct security problems. The guidelines also recommend 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.

157. The FTC also recommends 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 third-party service providers have implemented reasonable security measures.[43]

158. 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.

159. 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 failure to restrict access to information[44] and failure to segregate access to information[45] may violate the FTC Act.

---

[43] *See Start with Security*, FED. TRADE COMM'N, *supra* n.41.
[44] *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.
[45] *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).

160. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data (*i.e.*, Private Information), in all the specific ways alleged *infra* ¶ 170, constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

161. Furthermore, Defendants are 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.

162. The Security Rule requires Defendants 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

d. Ensure compliance by its workforce.[46]

163. Pursuant to HIPAA's mandate that Defendants follow "applicable standards, implementation specifications, and requirements . . . with respect to electronic protected health

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

information," 45 C.F.R. § 164.302, Defendants were 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).

164. Defendants are 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.

165. Both HIPAA and HITECH obligate Defendants 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.

166. In all the ways enumerated in Paragraph 170 below, Defendants failed to comply with HIPAA, HITECH, the FTC Act, and state laws including Section 501.171(2), Florida Statutes. They 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 Private Information.

D. Defendants Breached Their Duties to Plaintiffs and Class Members.

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

168. Furthermore, because Defendants collected and maintained Plaintiffs' and Class Members' Personal Information, and because Defendants were aware their participation in the healthcare industry rendered them—and, by extension, the customers whose data Defendants' aggregated and maintained—prime targets of cyber threats, Defendants were under a duty either to lessen the risk that Plaintiffs' and Class Members' Personal Information would be subject to a cyberattack, or to see that sufficient precautions were taken to protect Plaintiffs' and Class Members' Personal Information from the harm that the risk of a cyberattack posed.

169. As enumerated below, Defendants breached this duty of care to protect sensitive patient Private Information from reasonably foreseeable cyberattacks, including the Data Breach, and to see that sufficient precautions were taken to protect against the harm to Plaintiffs and Class Members that cyber threats posed to aggregated and collected Personal Information in Defendants' possession.

170. Defendants' specific negligent cybersecurity failures included, *inter alia*:

a. Failing to encrypt all sensitive patient Private Information;

b. Failing to implement hardened firewall rules, to blacklist traffic from and to IP addresses known to be malicious;

c. Failing to implement geo-blocking rules to sufficiently restrict access points into Defendants' server environment, so that, if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

d. Failing to enhance password complexity requirements and change administrative-level system accounts' passwords;

e. Failing to install patches to known vulnerabilities in their Citrix cloud software;

f. Failing to respond appropriately to warning, including from the FBI, that ransomware targeting Defendants' patient portal was available for sale on the dark web which they would have received as member of Health-ISAC;

g. Failing to detect and screen for threats in ingress and egress network traffic from international servers despite that Defendants' insureds entirely reside within the United States and would not ordinarily check dental insurance records or make a dental appointment from outside the United States, and despite the international nature of the organizations and threats faced;

h. Failing to include fail-safe features in their systems that, upon detecting unusual levels of international traffic, would have locked down and insulated their systems—and Plaintiffs' and Class Members' Personal Information—from cyber thefts such as the Data Breach;

i. Naming their domains and subdomains in ways that suggested they would likely contain patient Private Information, rather than storing all sensitive patient Private Information in subdomains with innocuous names;

j. Exposing third-party partner services (including Blackbaud, Inc., whose systems were previously compromised in a well-known data breach disclosed years before Defendants' Data Breach, in 2020) in its subdomains and links that may allow threat actors access by impersonating or compromising attached services and domains;

k. Failing to install sufficient system and security monitoring software across all their servers;

l. Failing to conduct database scanning and securing checks with sufficient frequency;

m. Failing to implement multi-factor authentication across computer systems,, especially where multi-factor authentication is an inexpensive, industry standard, and efficient tool widely available to Defendants to safeguard Plaintiffs' and Class Members' Private Information from cyberthreats, including the Data Breach;

n. Failing to require employees and contractors to change their passwords, and provide account holders with prompts to change their passwords, with sufficient frequency;

o. Failing to require employees to use passwords of sufficient complexity;

p. Failing to provide refresher HIPAA training to its active workforce with sufficient frequency;

q. Failing to issue laptops with sufficiently heightened security standards to all MCNA employees;

r. Failing to implement a threat management program to appropriate monitor Defendants' networks for external threats, and to assess, with sufficient frequency, whether monitoring tools are properly configured, tested, and updated; and

s. Failing to delete and purge the Private Information of Plaintiffs and Class Members no longer needed, such as of former insureds, and/or of medical information (*e.g.*, medicines, treatment information) past the statute-of-limitations for disputing a claim.

171. These failures, alone or in combination, constituted breaches of Defendants' duty of reasonable care to keep patient Private Information safe and secure from known cyberattack threats.

172. Indeed, Defendants were on notice that they were maintaining highly valuable data, which they 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.

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

174. Despite holding Private Information for almost more than 8.9 million individuals, Defendants 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.

175. As such, Defendants failed to properly implement data security practices that were reasonable and up to industry standards.

E. Defendants' Delay in Securing Their Systems and Notifying Its Customers of the Data Breach Caused Harm to Plaintiffs and Class Members.

176. Although Defendants' systems were first compromised on February 26, 2023, Defendants did not recognize their servers had been hacked until eight days later, on March 6, 2023.

177. Upon information and belief, Defendants failed to update their 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.

178. On May 3, 2023, 58 days after it discovered the theft of its Customers' highly sensitive Private Information, Defendants notified the Office of the Maine Attorney General that

8,923,662 individuals were affected by the Data Breach.[47]

179. Defendants also waited well over two months after they discovered their Customers' Private Information had been stolen before sending Notice Letters to individuals whose data was stolen in the Data Breach. While Defendants 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. MCNA's 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.[48]

180. The Notice Letter makes no mention the Data Breach involved a ransomware attack, of the ransom demanded by LockBit, or Defendants' refusal to pay even $1.12 per impacted

[47] 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).
[48] Ex. A; *see also* Ex. B (Notice Letter from "MCNA Dental" and Healthplex).

person (or less) to prevent LockBit from publishing Plaintiffs' and Class Members' highly sensitive Private Information.

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

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

F. The Data Breach Harmed Plaintiffs and Class Members.

183. Defendants' 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.

184. 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.

185. Cybercriminals sell PHI 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.[49] 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.

186. 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.[50]

187. According to the U.S. Government Accountability Office, "stolen data may be held 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."[51]

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

189. 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.

190. Identity thieves can use Private Information such as that exposed in the Data Breach

---

[49] *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).

[50] 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.

[51] *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).

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.

191. 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 billion stolen through bank account take-overs.[52]

192. The annual cost of identity theft is even higher. McAfee and the Center for Strategic and International Studies estimates the likely annual cost to the global economy from cybercrime is $445 billion a year.[53]

193. 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,

---

[52] *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 Sept. 4, 2024).

[53] *Facts + Statistics: Identity theft and cybercrime*, INSURANCE INFORMATION INSTITUTE, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last visited Sept. 4, 2024).

> remains the same.
>
> If you receive a new Social Security number, you shouldn't use the old number anymore.[54]

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.[55]

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

195. Moreover, cybercriminals need not harvest Plaintiffs' and Class Members' Social Security numbers 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.

196. 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 the identity theft they experienced

---

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

affected their ability to get credit cards and obtain loans such as student loans or mortgages.[56] 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.

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

198. The 2017 Identity Theft Resource Center survey[57] evidences the emotional suffering experienced by victims of identity theft:

- 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.

199. 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;

[56] *Identity Theft: The Aftermath 2017*, IDENTITY THEFT RESOURCE CENTER, https://www.idtheftcenter.org/wp-content/uploads/images/page-docs/Aftermath_2017.pdf (last visited Sept. 4, 2024).
[57] *Id.*

- 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.[58]

200. 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 from data breaches cannot necessarily rule out all future harm.[59]

201. 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:

a. losing the inherent value of their Private Information;

b. losing the value of Defendants' implicit promises of adequate data security;

c. identity theft and fraud resulting from the theft of their Private Information;

d. costs associated with the detection and prevention of identity theft and unauthorized use of their medical and health insurance information;

e. costs associated with purchasing credit monitoring and identity theft protection services;

f. 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

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

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;

g. lowered credit scores resulting from credit inquiries following fraudulent activities;

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

i. 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.

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

203. 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 Defendants would have no reason to tout their data security efforts to their actual and potential Customers.

204. Consequently, had Customers, including Plaintiffs and Class Members, known the truth about Defendants' data security practices—that the company would not adequately protect and store their data—they would not have entrusted their Private Information with Defendants, elected to receive health benefits that included Defendants' services, or paid for such services or

benefits. As such, Plaintiffs and Class Members did not receive the benefit of their bargain with Defendants because they paid for a value of services they expected but did not receive.

205. When Defendants announced the Data Breach to its Customers, they deliberately underplayed the Data Breach's severity, obfuscated the nature of the Data Breach, and offered only *de minimis* relief. Defendants merely offered Customers twelve months of free identity theft protection service and told them to "check your bills and accounts to be sure they look correct." [60] 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.

206. 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.

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

CLASS ACTION ALLEGATIONS

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

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

209. The Class asserts claims against Defendants for negligence (Count I); breach of implied contract (Count II); and for declaratory and injunctive relief under the Declaratory Judgment Act, 28 U.S.C. §§ 2201 *et seq.* (Count III).

[60] *See* Ex. A; Ex. B.

210. Excluded from the Class are Defendants, any entity in which Defendants have a controlling interest, and Defendants' 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 Defendants' counsel; members of the jury; and the legal representatives.

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

212. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Class 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, Defendants have acknowledged that the Private Information of at least 8,923,662 individuals throughout the United States and its territories was compromised in the Data Breach. Those persons' names and addresses are available from Defendants' 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.

213. **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 Defendants unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

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

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

d. Whether Defendants' data security systems were consistent with industry standards;

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

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

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

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

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

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

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

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

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

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

o. Whether Defendants' 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;

p. Whether, as a result of Defendants' 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;

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

214. **Typicality. Fed. R. Civ. P. 23(a)(3).** 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 Defendants' 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.

215. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiffs are adequate representatives of the Class because Plaintiffs are each members of the Class and are committed to pursuing this matter against Defendants to obtain relief for the Class. Plaintiffs have no conflicts of interest with the Class. 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 the Class.

216. **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 Defendants, and thus, individual litigation to redress Defendants' 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.

217. **Manageability**. **Fed. R. Civ. P. 23(b)(3).** The litigation of the class claims alleged herein is manageable. Defendants' 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.

218. **Ascertainability**. All members of the proposed Class are readily ascertainable. The Class is defined by reference to objective criteria, and there is an administratively feasible mechanism to determine who fits within the Class. Defendants have access to information

regarding which individuals were affected by the Data Breach and has already provided Data Breach notices to most of those people. Using this information, the Class Members can be identified, and their contact information ascertained for purposes of providing notice to the Class.

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

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

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

d. Whether implied contracts existed between Defendants (acting as insurers) on the one hand, and Plaintiffs and Class Members on the other, and the terms of those implied contracts;

e. Whether Defendants breached the implied contracts;

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

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

220. **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 Defendants to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

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

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

ii. requiring Defendants 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 Defendants to delete and purge the Private Information of Plaintiffs and Class Members unless Defendants 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 Defendants 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 Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis;

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

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

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

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

x. requiring Defendants 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 Defendants 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 Defendants' policies, programs, and systems for protecting personal identifying information;

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

xiii. requiring Defendants 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

COUNT I
NEGLIGENCE

221. Plaintiffs reallege and incorporate by reference the allegations contained in paragraphs 1 through 220 above, as if fully set forth herein.

222. Plaintiffs bring this claim on behalf of the Class against Defendants.

223. Defendants collected sensitive Private Information from Plaintiffs and Class Members as a requirement for using Defendants' products and services.

224. Defendants 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.

225. This duty included, among other things: (a) regularly designing, maintaining, and testing Defendants' security systems to ensure that Plaintiffs' and Class Members' Private

Information in Defendants' 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.

226. Defendants' duty to use reasonable care arose from several sources, including but not limited to those alleged herein.

227. Defendants 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.

228. Defendants' 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 Defendants. Only Defendants 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.

229. Defendants had every reason to know their 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. *See supra* ¶ 146 (detailing ransomware targeted to the MCNA patient portal for sale on the dark web since as early as 2019).

230. Defendants also had a duty to promptly notify Plaintiffs and Class Members of a breach because of state laws and statutes that require Defendants to reasonably safeguard sensitive Private Information, as alleged herein.

231. 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 Defendants' misconduct. Defendants were the only entities that had sufficient knowledge to properly provide this notice.

232. Defendants breached the duties they owed to Plaintiffs and Class Members alleged above and, thus, were negligent in so doing. Defendants 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 Defendants' possession had been or was reasonably believed to have been, stolen, or compromised.

233. More specifically, Defendants breached their duties of reasonable care by the following (alone or in combination):

a. Failing to encrypt all sensitive patient Private Information;

b. Failing to implement hardened firewall rules, to blacklist traffic from and to IP addresses known to be malicious;

c. Failing to implement geo-blocking rules to sufficiently restrict access points into Defendants' server environment, so that, if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

d. Failing to enhance password complexity requirements and change administrative-level system accounts' passwords;

e. Failing to install patches to known vulnerabilities in their Citrix cloud software;

f. Failing to respond appropriately to warning, including from the FBI, that ransomware targeting Defendants' patient portal was available for sale on the dark web which they would have received as member of Health-ISAC;

g. Failing to detect and screen for threats in ingress and egress network traffic from international servers despite that Defendants' insureds entirely reside within the United States and would not ordinarily check dental insurance records or make a dental appointment from outside the United States, and despite the international nature of the organizations and threats faced;

h. Failing to include fail-safe features in their systems that, upon detecting unusual levels of international traffic, would have locked down and insulated their systems—and Plaintiffs' and Class Members' Personal Information—from cyber thefts such as the Data Breach;

i. Naming their domains and subdomains in ways that suggested they would likely contain patient Private Information, rather than storing all sensitive patient Private Information in subdomains with innocuous names;

j. Exposing third-party partner services (including Blackbaud, Inc., whose

systems were previously compromised in a well-known data breach disclosed years before Defendants' Data Breach, in 2020) in its subdomains and links that may allow threat actors access by impersonating or compromising attached services and domains;

k. Failing to install sufficient system and security monitoring software across all their servers;

l. Failing to conduct database scanning and securing checks with sufficient frequency;

m. Failing to implement multi-factor authentication across computer systems,, especially where multi-factor authentication is an inexpensive, industry standard, and efficient tool widely available to Defendants to safeguard Plaintiffs' and Class Members' Private Information from cyberthreats, including the Data Breach;

n. Failing to require employees and contractors to change their passwords, and provide account holders with prompts to change their passwords, with sufficient frequency;

o. Failing to require employees to use passwords of sufficient complexity;

p. Failing to provide refresher HIPAA training to its active workforce with sufficient frequency;

q. Failing to issue laptops with sufficiently heightened security standards to all MCNA employees;

r. Failing to implement a threat management program to appropriate monitor Defendants' networks for external threats, and to assess, with sufficient frequency, whether monitoring tools are properly configured, tested, and updated; and

s. Failing to delete and purge the Private Information of Plaintiffs and Class Members no longer needed, such as of former insureds, and/or of medical information (*e.g.*,

medicines, treatment information) past the statute-of-limitations for disputing a claim.[61]

234. But for Defendants' negligent breaches of its duties owed to Plaintiffs and Class Members, their Private Information would not have been compromised.

235. Defendants' 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 and exploitation of Plaintiffs' and Class Members' Private Information.

236. Plaintiffs and Class Members were foreseeable victims of Defendants' inadequate data security practices, and it was also foreseeable that Defendants' 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.

237. As a direct and proximate result of Defendants' 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.

238. 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

[61] Plaintiffs in data breach cases are not required to "plead with exacting detail every aspect of [a defendant's] security history and procedures that might make a data breach foreseeable." *See Ramirez v. Paradies Shops, LLC*, 69 F.4th 1213, 1220-21 (11th Cir. 2023).

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 Defendants; (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 Defendants' 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
BREACH OF IMPLIED CONTRACT
(Against Defendants in Their Capacities As Insurers)

239. Plaintiffs reallege and incorporate by reference the allegations contained in paragraphs 1 through 220 above, as if fully set forth herein.

240. Plaintiffs bring this claim on behalf of the Class against Defendants in their capacities as insurers.

241. Defendants, acting in their capacities as insurers, offered to provide services to their Customers, including Plaintiffs and Class Members, in exchange for payment.

242. Defendants also required Plaintiffs and Class Members to provide them with their Private Information in order to receive services.

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

244. Plaintiffs and Class Members accepted Defendants' offer by providing their valuable PII and sensitive PHI to Defendants and their respective providers who in turn provided that information to Defendants in exchange for Plaintiffs and Class Members receiving

Defendants' services.

245. Plaintiffs and Class Members would not have done the foregoing but for the above-described agreements with the Defendants.

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

247. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendants, or such performance was waived by the Defendants' conduct.

248. However, Defendants breached the implied contracts they 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.

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

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

251. Defendants 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).

252. Defendants 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 PHI in violation of 45 C.F.R. § 164.306(a)(2).

253. As a direct and proximate result of Defendants' above-alleged breach of implied contract, Plaintiffs and Class Members have suffered (and will continue to suffer) 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 Defendants; (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 Defendants' 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.

254. Accordingly, Plaintiffs and the Class are entitled to damages in an amount to be determined at trial, including actual, consequential, and nominal damages.

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

255. Plaintiffs reallege and incorporate by reference the allegations contained in paragraphs 1 through 220 above, as if fully set forth herein.

256. Plaintiffs bring this claim on behalf of the Class against Defendants.

257. 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.

258. Defendants owed a duty of care to Plaintiffs and Class Members, which required them to adequately monitor and safeguard Plaintiffs' and Class Members' Private Information.

259. Defendants still possess the Private Information belonging to Plaintiffs and Class Members.

260. Plaintiffs allege Defendants' 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.

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

a. Defendants owe 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. Defendants' 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. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure Plaintiffs' and Class Members' Private Information.

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

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

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

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

ii. requiring Defendants 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 Defendants to delete and purge the Private Information of Plaintiffs and Class Members unless Defendants 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 Defendants 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 Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis;

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

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

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

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

x. requiring Defendants 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 Defendants 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 Defendants' policies, programs, and systems for protecting personal identifying information;

xii. requiring Defendants to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor Defendants' networks for internal and external threats, and assess whether monitoring tools are

properly configured, tested, and updated; and

xiii. requiring Defendants to meaningfully educate all Class Members about the threats they face 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.

263. If an injunction is not issued, Plaintiffs will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach of Defendants' 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.

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

265. Issuance of the requested injunction will serve the public interest. Such an injunction would benefit the public by preventing a subsequent data breach of Defendants' systems and network, thus preventing future injury to Plaintiffs and other Class Members whose Private Information would be further compromised.

266. 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 Defendants.

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 Defendants breached their duties to Plaintiffs and Class Members;

C. A mandatory injunction directing Defendants 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 Defendants 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 award of damages, including actual, nominal, consequential damages, as allowed by law in an amount to be determined;

F. An award of pre- and post-judgment interest, costs, attorneys' fees, expenses, and interest as permitted by law;

G. For all other orders, findings, and determinations identified and sought in this Complaint; and

H. 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: September 13, 2024.

Respectfully Submitted,

By: *Jeff Ostrow*
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

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

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 13th day of September, 2024.

*/s/ Jeff Ostrow*_____
Jeff Ostrow