# Exhibit A

**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,**

Defendant.

# 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"). The following allegations are based upon Plaintiffs' personal knowledge as to their own actions and their counsels' investigations, facts of public record, and upon information and belief as to all other matters.

1. This action arises from MCNA's 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 and State Subclasses (defined *infra* ¶¶ 198, 200) for whom MCNA performed services.

2. MCNA is one of the largest government-sponsored dental insurance providers in

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

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

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

[1] https://www.mcna.net/en/company-overview (last visited Nov. 11, 2023).

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

[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).

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

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

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

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

9. Taking reasonable, standard precautions against cybercrime and data breaches is a

[4] *Id.*
[5] *Id.*
[6] *Id.*

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

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

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

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

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

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

[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.

[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.

$1,300 each on the black market.[9]

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

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

18. Furthermore, as described in detail *infra* ¶¶ 137-41, the known modus operandi of the LockBit ransomware group puts Plaintiffs and Class Members at a much higher likelihood of ongoing risk. LockBit is well known to perform retaliatory "data dumps" of stolen information when corporate victims of its data breach activities refuse to pay their extortion demands. Indeed, they operate a notorious data breach "dump site" on the dark web where they make Plaintiffs' and Class Members' data available to anyone who cares to take it as a method of both punishing those who do not pay and as a means to validate their threats to future victims.

19. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have suffered actual and present injuries, including but not limited to: (a) present and continuing threats of identity theft crimes, fraud, scams, and other misuses of their Private Information; (b) diminution of value of their Private Information; (c) loss of benefit of the bargain (price premium damages); (d) loss of value of privacy and confidentiality of the stolen Private Information; (e) illegal sales of the compromised Private Information; (f) mitigation expenses and time spent on

[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-idUSKBN0GK24U20140820.

credit monitoring; (g) identity theft insurance costs; (h) "out of pocket" costs incurred due to actual identity theft; (i) credit freezes/unfreezes; (j) expense and time spent on initiating fraud alerts and contacting third parties; (k) decreased credit scores; (l) lost work time; (m) anxiety, annoyance, and nuisance; and (n) continued risk to their Private Information, which remains in MCNA's possession and is subject to further breaches so long as MCNA fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

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

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

## JURISDICTION AND VENUE

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

23. This Court has personal jurisdiction over MCNA because its headquarters and principal place of business is in Fort Lauderdale, Florida.

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

## PARTIES

### Plaintiff, Agustin Acosta

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

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

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

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

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

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

lifetime.

**Plaintiff, Brittney Brown**

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

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

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

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

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

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

**Plaintiff, Montwain Carter**

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

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

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

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

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

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

**Plaintiff, Donna Crowe**

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

of Florida.

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

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

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

47. As a direct and proximate result of the Data Breach, Plaintiff Crowe has made reasonable efforts to mitigate the impact of the Data Breach, including calling her credit union regarding the Data Breach and regularly checking her bank and credit card statements for fraud.

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

**Plaintiff, Shavonne Diggs**

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

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

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

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

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

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

**Plaintiff, Crystal Gannon**

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

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

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

58. Plaintiff Gannon was a victim of identity theft following the Data Breach. After the

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

59. As a direct and proximate result of the Data Breach, Plaintiff Gannon has made reasonable efforts to mitigate the impact of the Data Breach, including by researching the Data Breach, regularly and closely monitoring her financial accounts, and placing a credit freeze through Experian.

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

**Plaintiff, Yvon Hanekom**

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

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

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

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

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

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

**Plaintiff, Samantha Hathaway**

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

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

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

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

71. As a direct and proximate result of the Data Breach, Plaintiff Hathaway has made reasonable efforts to mitigate the impact of the Data Breach. She regularly checks all her financial, health, and insurance accounts. She has also changed the passwords for her financial and other accounts, cancelled her bank and credit cards, and ordered new cards.

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

**Plaintiff, Sara Hughes**

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

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

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

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

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

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

**Plaintiff, Tarek Kachakech**

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

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

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

82. Since the Data Breach, Plaintiff Kachakech has experienced an increased number of phishing calls and spam text messages. Also, his Facebook account was hacked and subsequently disabled by Facebook. He is anxious and fearful he will continue to experience

identity theft in the future because of the Data Breach. He is also suffering emotionally after his Facebook account was hacked because he lost all his contacts and connections.

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

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

**Plaintiff, Kade McCraw**

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

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

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

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

could negatively affect his credit score and prevent him from owning a home.

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

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

**Plaintiff, Heather Shaffer**

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

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

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

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

psychiatrist for increased anxiety following the Data Breach. She is concerned about the violation of her privacy rights, identity theft, and having to rebuild her credit if that happens.

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

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

**Plaintiff, Aliciah Souza-Shores**

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

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

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

100. Since the Data Breach, Plaintiff Souza-Shores had to close her debit card and open a new one after unauthorized charges appeared on it, has received alerts from Kroll about suspicious activity on her accounts and that her confidential information is on the dark web, and became aware of an attempt to open an account in her name. As a result of the canceled card, she spent considerable time resetting all her automatic payments, including her mortgage payments, and incurred late fees on her mortgage and water bill. In addition, she has noticed inquiries on her credit report that were not initiated by her. Moreover, she has noticed a marked increase in phishing

emails, spam texts asking her to respond, and telephone calls asking her to press a number to continue. She has been experiencing anxiety as a result of the Data Breach and spends an hour each day trying to relax and not worry about it. She is concerned about the risk of identity theft and the privacy of her HIPAA-protected information.

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

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

**Plaintiff, Asia Spears**

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

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

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

106. Plaintiff Spears was the victim of identity theft following the Data Breach. On or about September 2023, a credit card was opened in her name with a $1,000 credit limit. Additionally, there were several unauthorized transactions in her bank account that caused the account to overdraft by $900. Also, an unauthorized $1,200 transaction appeared on her CashApp. She is out-of-pocket for these losses and the bank closed her account. Plaintiff Spears has also

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

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

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

**Plaintiff, Heidi Winkler**

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

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

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

112. Plaintiff Winkler was the victim of identity theft following the Data Breach. She had to cancel her debit card and have a new debit card issued due to the card being used for multiple

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

113. As a direct and proximate result of the Data Breach, Plaintiff Winkler has made reasonable efforts to mitigate the impact of the Data Breach. Dealing with the consequences of the Data Breach has become a daily occurrence for Plaintiff Winkler, who receives multiple spam calls each day, along with spam text messages. She has spent time addressing the Data Breach, including having to cancel her debit card after it was used for unauthorized purposes.

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

**Plaintiff, Franny Zurline**

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

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

117. Plaintiff Zurline received a Notice Letter from MCNA dated May 26, 2023,

concerning the Data Breach.

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

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

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

**Defendant**

121. MCNA is a corporation organized and validly existing under the laws of Florida, with its current principal place of business located at 7901 SW 6th Ct., Suite 400, Plantation, Florida 33309.

## FACTUAL ALLEGATIONS

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

122. 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 offers dental plans for private employers, individuals, and families.[12]

123. "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]

124. MCNA collects and processes an enormous volume of personal data from millions of Customers, including Private Information like health and patient records, insurance information, and financial information. Some of this information is not provided to MCNA directly, but through Medicaid, CHIP, or Medicare.

125. MCNA's website contains a Notice of Privacy Practices, in which MCNA 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."[14] MCNA also claims it is "committed to complying with the requirements and standards of the Health Insurance Portability and Accountability Act of 1996 (HIPAA)."[15] The Notice of Privacy Practices explicitly states it "applies to all MCNA dental programs that are administered by" MCNA.[16]

126. MCNA states it must follow the privacy practices in its Notice of Privacy Practices.[17]

127. MCNA claims to protect PHI, including medical information and other PII like names, addresses, telephone numbers, and Social Security numbers, "in all formats including

[11] *Company Overview*, MCNA, https://www.mcna.net/en/company-overview (last visited Nov. 11, 2023).
[12] *Id.*
[13] *Home*, MCNA, https://www.mcna.net/en/home (last visited Nov. 11, 2023).
[14] *Our Privacy Practices*, MCNA, https://www.mcna.net/en/privacy (last visited Nov. 11, 2023).
[15] *Id.*
[16] *Id.*
[17] *Id.*

electronic, written and oral information."[18]

128. MCNA acknowledges that "[t]he law says MCNA has to keep your health information private."[19] 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."[20]

129. 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."[21] The Notice of Privacy Practices lists several ways that MCNA may use its Customers' information, including, *inter alia*, for research, to comply with the law, and to address workers' compensation claims.[22]

130. MCNA promises to "let you know promptly if a breach occurs that may have compromised the privacy or security of your information."[23]

131. 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.

132. 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."[24] MCNA's website also states that "DentalTrac™ is hosted across multiple geographically dispersed, military grade, secure, and state-of-the-art data centers" and that the system "has been

[18] *Id.*
[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] *Id.*
[23] *Id.*
[24] *Company Overview*, *supra* n.11.

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."[25]

133. Plaintiffs and Class Members relied on MCNA's promise to keep their Private Information confidential and securely maintained, and to only make authorized disclosures of this information. MCNA failed to do so.

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

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

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

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

137. The notorious LockBit ransomware gang claimed responsibility for the

[25] *Our Technology*, MCNA, https://www.mcna.net/en/technology/ (last visited Nov. 11, 2023).

[26] *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").

cyberattack.[27] LockBit is one of the most active ransomware actors, having breached over 1,000 companies worldwide.[28] 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.[29] 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.

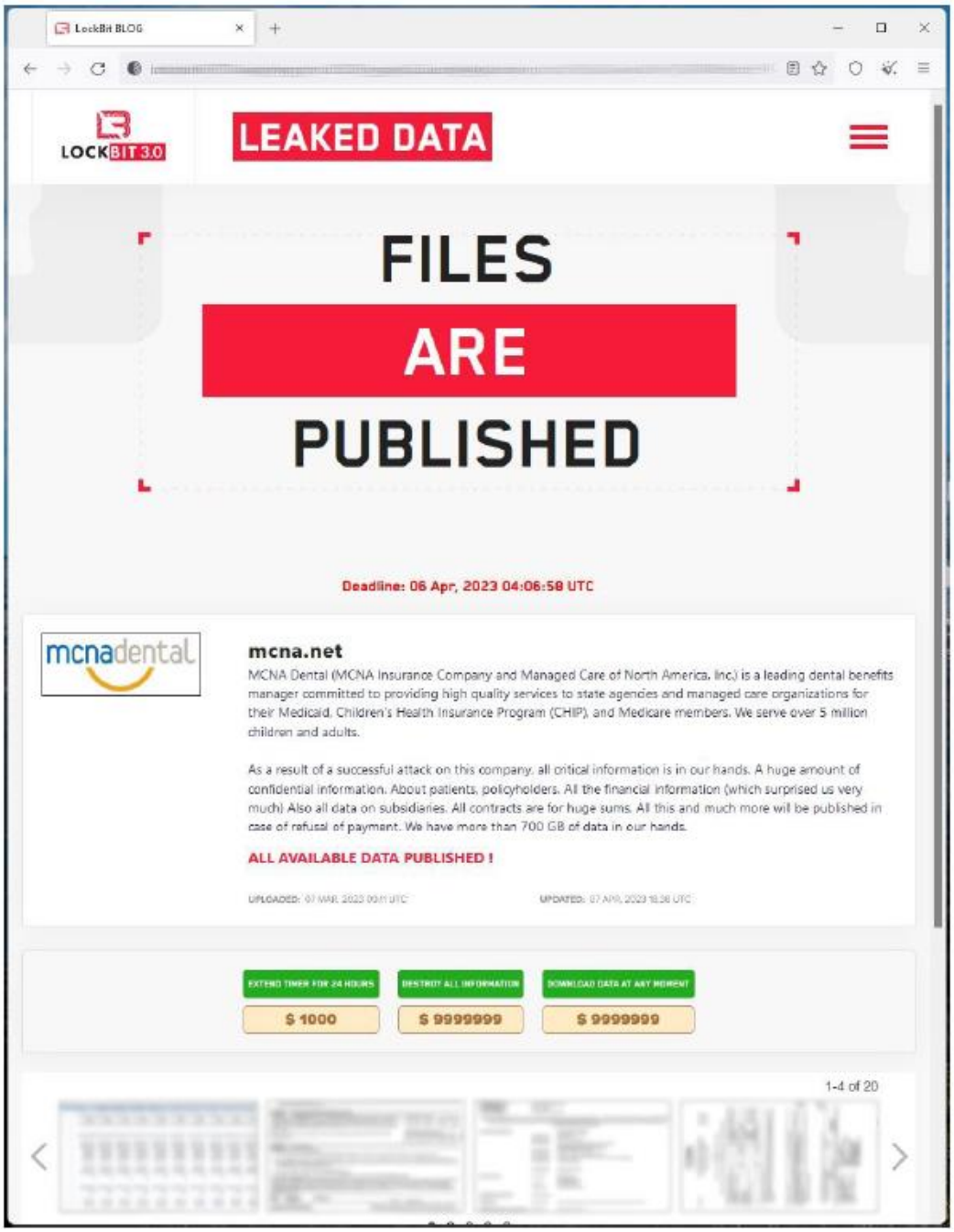
138. MCNA, a self-proclaimed "leader" in the dental benefits industry, knew or should have known of the tactics that groups like LockBit employ.

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

[27] 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.

[28] 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.

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




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

site and has been exposed for theft and sale on the dark web. This information will remain on the site indefinitely, causing ongoing risk and continuing harms to plaintiffs.

141. LockBit's history[30] makes the disclosure of Plaintiffs' and Class Members' Private Information to illegal operators a near certainty.[31]

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

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

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

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

---

[30] 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).

[31] "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).

145. On May 3, 2023, 58 days after it discovered the theft of its Customers' highly sensitive Private Information, MCNA notified the Office of the Maine Attorney General that 8,923,662 individuals were affected by the Data Breach.[32]

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

> **What happened?**
> On March 6, 2023, MCNA became aware of certain activity in our computer system that happened without our permission. We quickly took steps to stop that activity. We began an investigation right away. A special team was hired to help us. We learned a cybercriminal was able to see and take copies of some information in our computer system between February 26, 2023 and March 7, 2023.
>
> **What information may have been involved?**
> On May 4, 2023, we told the state Medicaid agency that this event may have involved your information. Here is the list of information that was seen and taken:
>
> - Information used to contact you, like first and last name, address, date of birth, telephone number, email
> - Social Security number
> - Driver's license number/other government-issued ID number
> - Health insurance (plan information, insurance company, member number, Medicaid-Medicare ID numbers)
> - Care for teeth or braces (visits, dentist name, doctor name, past care, x-rays/photos, medicines, and treatment)
> - Bills and insurance claims
>
> Some of this information was for a parent, guardian, or guarantor. A guarantor is the person who paid the bill. Information which was seen and taken was not the same for everyone.[33]

[32] 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-b0415575de 56.shtml (last visited Nov. 11, 2023).

[33] Ex. A.

147. MCNA's Notice Letter makes no mention the Data Breach involved a ransomware attack, of the ransom demanded by LockBit, or MCNA's refusal to pay even $1.12 per impacted person (or less) to prevent LockBit from publishing Plaintiffs' and Class Members' highly sensitive Private Information.

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

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

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

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

151. 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.

152. MCNA was fully aware the healthcare benefits industry is a prime target for cyber threats.[34] 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

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

patients, March 2022). Between 2020 and 2021, attacks on the healthcare industry increased 71%, making it the fifth most common industry targeted by cyberattacks.[35]

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

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

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

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

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

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

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

158. Federal and state regulators have established security standards and issued

[35] 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.

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.

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

160. 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.[36]

161. 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.[37]

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

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

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

for business.[38] The guidelines note businesses should protect the personal customer information that they keep; properly dispose of Private Information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

163. The FTC also recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[39]

164. 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.

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

[38] *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).

[39] *See Start with Security*, FED. TRADE COMM'N, *supra* n.37.

failure to restrict access to information[40] and failure to segregate access to information[41] may violate the FTC Act.

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

167. Furthermore, MCNA is required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C. The Privacy Rule and the Security Rule set nationwide standards for protecting health information, including health information stored electronically.

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

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

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

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

[40] *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.

[41] *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 258 (3d Cir. 2015) (stating that companies should use "readily available security measures to limit access between" data storage systems).

d. Ensure compliance by its workforce.[42]

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

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

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

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

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

**G. The Data Breach Harmed Plaintiffs and Class Members.**

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

174. 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.

175. Cyber criminals sell health information at a far higher premium than stand-alone PII. This is because health information enables thieves to go beyond traditional identity theft and obtain medical treatments, purchase prescription drugs, submit false bills to insurance companies, or even undergo surgery under a false identity.[43] 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.

176. 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.[44]

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

[43] *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).

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

for up to a year or more before being used to commit identity theft," and "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years."[45]

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

179. 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.

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

181. 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

[45] *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/GAOREPORTSGAO-07-737.htm (last visited Nov. 11, 2023).

billion stolen through bank account take-overs.[46]

182. The annual cost of identity theft is even higher. McAfee and the Center for Strategic and International Studies estimates that the likely annual cost to the global economy from cybercrime is $445 billion a year.[47]

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

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

For some victims of identity theft, a new number actually creates new problems. If the old credit card information is not associated with the new number, the absence of any credit history under the new number may make it more difficult to get credit.[48]

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

---

[46] *2018 Identity fraud: Fraud Enters a New Era of Complexity*, JAVELIN, https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity (last visited Nov. 11, 2023).

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

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

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

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

186. And, the impact of identity theft can have ripple effects, which can adversely affect the future financial trajectories of victims' lives. For example, the Identity Theft Resource Center reports that respondents to their surveys in 2013-2016 described that the identity theft they experienced affected their ability to get credit cards and obtain loans such as student loans or mortgages.[49] 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.

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

188. The 2017 Identity Theft Resource Center survey[50] evidences the emotional suffering experienced by victims of identity theft:

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

[50] *Id*.

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

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

- 48.3% of respondents reported sleep disturbances;
- 37.1% reported an inability to concentrate / lack of focus;
- 28.7% reported they were unable to go to work because of physical symptoms;
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues); and
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[51]

190. 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

[51] *Id.*

from data breaches cannot necessarily rule out all future harm.[52]

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

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

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

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

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

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

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

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

195. When MCNA announced the Data Breach to its Customers, it deliberately underplayed the Data Breach's severity, obfuscated the nature of the Data Breach, and offered only *de minimis* relief. MCNA merely offered its Customers 12 months of free identity theft protection service and told them to "check your bills and accounts to be sure they look correct." [53] 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.

[53] *See* Ex. A.

196. 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.

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

## CLASS ACTION ALLEGATIONS

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

**Nationwide Class**

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

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

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

**Alabama Subclass**

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

**Arkansas Subclass**

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

**Florida Subclass**

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

**Idaho Subclass**

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

**Iowa Subclass**

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

**Louisiana Subclass**

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

**Massachusetts Subclass**

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

**Mississippi Subclass**

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

**or about February 26, 2023.**

**Nebraska Subclass**

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

**New York Subclass**

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

**Texas Subclass**

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

**Utah Subclass**

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

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

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

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

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

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

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

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

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

standards;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

manageability problems with prosecuting this lawsuit as a class action.

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

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

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

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

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

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

e. Whether MCNA breached the implied contract;

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

g. Whether MCNA failed to implement and maintain reasonable security

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

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

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

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

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

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

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

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

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

privacy interests of Plaintiffs and Class Members;

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

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

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

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

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

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

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

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

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

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

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

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

## CAUSES OF ACTION

## ON BEHALF OF THE NATIONWIDE CLASS, OR ALTERNATIVELY, ON BEHALF OF THE STATE SUBCLASSES

### COUNT I
### NEGLIGENCE

212. Plaintiffs reallege and incorporate by reference the allegations contained in paragraphs 1 through 211 above, as if fully set forth herein.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## COUNT II
## NEGLIGENCE *PER SE*

229. Plaintiffs reallege and incorporate by reference the allegations contained in paragraphs 1 through 211 above, as if fully set forth herein.

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

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

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

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

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

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

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

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

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

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

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

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

240. Plaintiffs reallege and incorporate by reference the allegations contained in paragraphs 1 through 211 above, as if fully set forth herein.

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

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

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

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

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

described agreement with the company.

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

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

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

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

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

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

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

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

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

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

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

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

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

## COUNT IV
## UNJUST ENRICHMENT

258. Plaintiffs reallege and incorporate by reference the allegations contained in paragraphs 1 through 211 above, as if fully set forth herein.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

271. Plaintiffs have no adequate remedy at law.

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

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

273. Plaintiffs reallege and incorporate by reference the allegations contained in paragraphs 1 through 211 above, as if fully set forth herein.

274. 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.

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

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

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

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

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

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

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

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

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

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

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

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

alleged herein;

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

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

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

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

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

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

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

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

traffic;

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

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

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

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

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

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

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

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

## CLAIM ON BEHALF OF THE ALABAMA SUBCLASS

### COUNT VI
### ALABAMA DECEPTIVE TRADE PRACTICES ACT
### Ala. Code §§ 8-19-1 *et seq.*

284. Plaintiff Hanekom (for the purposes of this count, "Plaintiff") realleges and incorporates by reference the allegations contained in paragraphs 1 through 211 above, as if fully set forth herein.

285. Plaintiff brings this claim on behalf of himself and the Alabama Subclass.

286. MCNA is a "person" as defined by Ala. Code § 8-19-3(10).

287. Plaintiff and Alabama Subclass Members are "consumers" as defined by Ala. Code § 8-19-3(4).

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

289. MCNA engaged in deceptive acts and practices in the conduct of trade or commerce, in violation of the Alabama Deceptive Trade Practices Act, Ala. Code § 8-19-5, including:

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or qualities that they do not have or that a person has sponsorship, approval, status, affiliation, or connection that he or she does not have;

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

c. Engaging in any other unconscionable, false, misleading, or deceptive act or practice in the conduct of trade or commerce, including acts and practices that would violate Section 5(a)(1) of the FTC Act, as interpreted by the FTC and federal courts, and/or HIPAA, the HIPAA Privacy Rule and Security Rule, and HITECH.

290. MCNA's deceptive acts and practices include:

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

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

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

Data Breach Notification Act of 2018, Ala. Cod. § 8-38-1, which was a direct and proximate cause of the Data Breach;

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

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 45 C.F.R. § 164, and the Alabama Data Breach Notification Act of 2018, Ala. Cod. § 8-38-1;

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

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 45 C.F.R. § 164, and the Alabama Data Breach Notification Act of 2018, Ala. Cod. § 8-38-1.

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

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

293. Had MCNA disclosed to Plaintiff and Alabama Subclass Members that its data

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

294. MCNA acted intentionally, knowingly, and maliciously to violate the Alabama Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Alabama Subclass Members' rights.

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

296. MCNA's deceptive acts and practices caused substantial injury to Plaintiff and Alabama Subclass Members, which they could not reasonably avoid, and which outweighed any benefits to consumers or to competition.

297. Plaintiff and the Alabama Subclass seek all monetary and non-monetary relief

allowed by law, including, pursuant to § 8-19-10(1) the greater of (a) actual damages or (b) statutory damages of $100; treble damages; injunctive relief; attorneys' fees, costs, and any other relief that is just and proper.

## CLAIM ON BEHALF OF THE ARKANSAS SUBCLASS

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

298. Plaintiff Gannon (for the purposes of this count, "Plaintiff") realleges and incorporates by reference the allegations contained in paragraphs 1 through 211 above, as if fully set forth herein.

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

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

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

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

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

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

a. Knowingly making a false representation as to the characteristics,

ingredients, uses, benefits, alterations, source, sponsorship, approval, or certification of goods or services or as to whether goods are original or new or of a particular standard, quality, grade, style, or model;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

discovered.

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

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

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

## CLAIM ON BEHALF OF THE FLORIDA SUBCLASS

### COUNT VIII
### FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT
### Fla. Stat. §§ 501.201 *et seq.*

312. Plaintiff Crowe, Plaintiff Spears, and Plaintiff Winkler (for the purposes of this count, "Plaintiffs") reallege and incorporate by reference the allegations contained in paragraphs 1 through 211 above, as if fully set forth herein.

313. Plaintiffs bring this claim on behalf of themselves and the Florida Subclass.

314. Plaintiffs and Florida Subclass Members are "consumers" as defined by Fla. Stat. § 501.203.

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

316. MCNA engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1), including:

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

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

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Florida Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 45 C.F.R. § 164, and Florida's data security statute, F.S.A. § 501.171(2), which was a direct and proximate cause of the Data Breach;

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

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

C.F.R. § 164, and Florida's data security statute, F.S.A. § 501.171(2);

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

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Florida Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 45 C.F.R. § 164, and Florida's data security statute, F.S.A. § 501.171(2).

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

318. MCNA intended to mislead Plaintiffs and Florida Subclass Members and induce them to rely on its misrepresentations and omissions.

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

320. As a direct and proximate result of MCNA's unconscionable, unfair, and deceptive acts and practices, Plaintiffs and Florida Subclass Members have suffered and will continue to

suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as alleged herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial and other accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for MCNA's services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

321. Plaintiffs and Florida Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages under Fla. Stat. § 501.211; declaratory and injunctive relief; reasonable attorneys' fees and costs, under Fla. Stat. § 501.2105(1); and any other relief that is just and proper.

## CLAIM ON BEHALF OF THE IDAHO SUBCLASS

### COUNT IX
### IDAHO CONSUMER PROTECTION ACT
### Idaho Code §§ 48-601 *et seq.*

322. Plaintiff Zurline (for the purposes of this count, "Plaintiff") realleges and incorporates by reference the allegations contained in paragraphs 1 through 211 above, as if fully set forth herein.

323. Plaintiff brings this claim on behalf of herself and the Idaho Subclass.

324. MCNA is a "person" as defined by Idaho Code § 48-602(1).

325. MCNA's conduct described herein pertained to "goods" and "services" as defined by Idaho Code §§ 48-602(6) and (7).

326. MCNA engaged in unfair, deceptive, and unconscionable trade practices, in the conduct of trade and commerce with respect to the sale and advertisement of goods and services, in violation of Idaho Code §§ 48-603 and 48-603(C), including:

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

b. Representing that good are of a particular standard, quality, or grade when they are of another;

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

d. Engaging in other acts and practices that are otherwise misleading, false, or deceptive to consumers; and

e. Engaging in unconscionable methods, acts or practices in the conduct of trade or commerce.

327. MCNA's unfair, deceptive, and unconscionable acts and practices include:

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

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

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

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

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

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

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

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

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

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

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

332. Plaintiff and Idaho Subclass Members seek all monetary and non-monetary relief allowed by law, including damages; punitive damages; injunctive relief; attorneys' fees and costs; and any other relief that is just and proper.

## CLAIMS ON BEHALF OF THE IOWA SUBCLASS

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

333. Plaintiff Carter (for the purposes of this count, "Plaintiff") realleges and incorporates by reference the allegations contained in paragraphs 1 through 211 above, as if fully set forth herein.

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

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

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

337. MCNA is required to accurately notify Plaintiff and Iowa Subclass Members if it

becomes aware of a breach of its data security system "in the most expeditious manner possible and without unreasonable delay." Iowa Code § 715C.2(1).

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

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

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

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

## COUNT XI
## IOWA CONSUMER FRAUDS ACT
## Iowa Code § 714H

342. Plaintiff Carter (for the purposes of this count, "Plaintiff") realleges and incorporates by reference the allegations contained in paragraphs 1 through 211 above, as if fully set forth herein.

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

344. MCNA is a "person" as defined by Iowa Code § 714H.2(7).

345. Plaintiff and Iowa Subclass Members are "consumers" as defined by Iowa Code § 714H.2(3).

346. MCNA's conduct described herein related to the "sale" or "advertisement" of "merchandise" as defined by Iowa Code §§ 714H.2(2), (6), and (8).

347. MCNA engaged in unfair, deceptive, and unconscionable trade practices, in violation of the Iowa Consumer Frauds Act ("ICFA"), including:

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

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

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

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

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

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

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

Plaintiff's and Iowa Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA, 45 C.F.R. § 164.

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

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

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

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

352. Plaintiff has provided the requisite notice to the Iowa Attorney General, the office of which approved the filing of this class action lawsuit pursuant to Iowa Code § 714H.7.

353. Plaintiff and Iowa Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages; punitive damages; injunctive relief; reasonable attorneys' fees and costs; and any other relief that is just and proper.

## CLAIMS ON BEHALF OF THE LOUISIANA SUBCLASS

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

354. Plaintiff Diggs and Plaintiff Souza-Shores (for the purposes of this count, "Plaintiffs") reallege and incorporate by reference the allegations contained in paragraphs 1 through 211 above, as if fully set forth herein.

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

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

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

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

359. Because MCNA was aware of a breach in its security systems as of March 6, 2023, it had a duty to disclose the Data Breach in a timely and accurate fashion as mandated by La. Rev.

Stat. § 51:3074(C). MCNA failed to do so, waiting until late May 2023 to publish a data breach notification on its website.

360. As a direct and proximate result of MCNA's violations of La. Rev. Stat. § 51:3074(C), Plaintiffs and Louisiana Subclass Members suffered damages, as described above.

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

## COUNT XIII
## LOUISIANA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW
## La. Rev. Stat. §§ 51:1401 *et seq.*

362. Plaintiff Diggs and Plaintiff Souza-Shores (for the purposes of this count, "Plaintiffs") reallege and incorporate by reference the allegations contained in paragraphs 1 through 211 above, as if fully set forth herein.

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

364. The Louisiana Unfair Trade Practices and Consumer Protection Law, La Rev. Stat. §§ 51:1401 *et seq.* ("LUPTA") makes unlawful "[u]nfair methods of competition and unfair or deceptive act or practices in the conduct of any trade or commerce." La. Rev. Stat. § 51:1405(A). Unfair acts are those that offend established public policy, while deceptive acts are those that amount to fraud, deceit, or misrepresentation.

365. MCNA is a "person" as defined by LUPTA. La. Rev. Stat. § 51:1402(1).

366. MCNA engaged in "trade" or "commerce" within the meaning of La. Rev. Stat. § 51:1402(10).

367. MCNA participated in unfair and deceptive acts and practices that violated LUPTA, including:

a. Failing to implement and maintain reasonable security and privacy

measures to protect Plaintiffs' and Louisiana Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

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

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Louisiana Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 45 C.F.R. § 164, and Louisiana's data security statute, La. Rev. Stat. § 51:3074, which was a direct and proximate cause of the Data Breach;

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

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Louisiana Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 45 C.F.R. § 164, and Louisiana's data security statute, La. Rev. Stat. § 51:3074;

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

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

security statute, La. Rev. Stat. § 51:3074.

368. MCNA's conduct was not only deceptive, but also unfair within the meaning of LUPTA because it constitutes immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or competition. The injuries suffered by Plaintiffs and the Louisiana Subclass are not outweighed by any countervailing benefits to consumers or competition. Because MCNA is solely responsible for securing its networks and protecting Private Information, there is no way Plaintiffs and Louisiana Subclass Members could have known about MCNA's inadequate data security practices or avoided the injuries they sustained. There were reasonably available alternatives to further MCNA's legitimate business interests, other than its conduct responsible for the Data Breach.

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

370. MCNA intended to mislead Plaintiffs and Louisiana Subclass Members and induce them to rely on its misrepresentations and omissions.

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

discovered.

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

373. Plaintiffs and Louisiana Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages; treble damages for MCNA's knowing violations of LUPTA; injunctive relief; reasonable attorneys' fees and costs; and any other relief that is just and proper.

## CLAIM ON BEHALF OF THE MASSACHUSETTS SUBCLASS

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

374. Plaintiff McCraw (for the purposes of this count, "Plaintiff") realleges and incorporates by reference the allegations contained in paragraphs 1 through 211 above, as if fully set forth herein.

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

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

377. MCNA operates in "trade or commerce" as meant by Mass. Gen. Laws Ann. Ch.

93A § 1(b).

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

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

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

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

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

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

e. Misrepresenting that they would comply with common law and statutory

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

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

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 45 C.F.R. § 164, and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05.

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

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

382. Had MCNA disclosed to Plaintiff and Massachusetts Subclass Members that its data systems were not secure and, thus, were vulnerable to attack, MCNA would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. MCNA was trusted with sensitive and valuable Private Information

regarding millions of consumers, including Plaintiff and Massachusetts Subclass Members. MCNA accepted the responsibility of protecting the data but kept the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Massachusetts Subclass Members acted reasonably in relying on MCNA's misrepresentations and omissions, the truth of which they could not have discovered.

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

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

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

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

**CLAIM ON BEHALF OF THE MISSISSIPPI SUBCLASS**

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

387. Plaintiff Brown (for the purposes of this count, "Plaintiff") realleges and incorporates by reference the allegations contained in paragraphs 1 through 211 above, as if fully set forth herein.

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

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

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

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

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

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

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

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

maintaining reasonable security measures;

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

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

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 45 C.F.R. § 164, and Miss. Code. Ann. § 75-24-29.

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

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

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

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

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

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

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

396. MCNA had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extensivity of the Private Information in its possession, and the generally accepted professional standards. Such a duty is implied by law due to the nature of the relationship between consumers-including Plaintiff and the Mississippi Subclass and MCNA. MCNA's duty to disclose also arose from its:

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

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

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

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

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

399. MCNA's violations present a continuing risk to Plaintiff and Mississippi Subclass Members as well as to the general public.

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

## CLAIMS ON BEHALF OF THE NEBRASKA SUBCLASS

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

401. Plaintiff Shaffer (for the purposes of this count, "Plaintiff") realleges and incorporates by reference the allegations contained in paragraphs 1 through 211 above, as if fully set forth herein.

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

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

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

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

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

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

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

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

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

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

Plaintiff's and Nebraska Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA, 45 C.F.R. § 164.

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

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

407. MCNA's conduct was not only deceptive, but also unfair within the meaning of NCPA because it constitutes immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or competition. The injuries suffered by Plaintiff and the Nebraska Subclass are not outweighed by any countervailing benefits to consumers or competition. Because MCNA is solely responsible for securing its networks and protecting Private Information, there is no way Plaintiff and Nebraska Subclass Members could have known about MCNA's inadequate data security practices or avoided the injuries they sustained. There were reasonably available alternatives to further MCNA's legitimate business interests, other than its conduct responsible for the Data Breach.

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

services made necessary by the Data Breach.

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

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

410. Plaintiff Shaffer (for the purposes of this count, "Plaintiff") realleges and incorporates by reference the allegations contained in paragraphs 1 through 211 above, as if fully set forth herein.

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

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

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

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

415. MCNA knowingly made false or misleading statements in its Notice of Privacy Practices regarding the use of personal information submitted by Customers, in that it did not "safeguard[] [its] members' protected health information" and protect "individually identifiable information, like your name, address, telephone number, [and] Social Security number"[54] in violation of Neb. Rev. Stat. § 87-302(a)(15).

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

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

## CLAIMS ON BEHALF OF THE NEW YORK SUBCLASS

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

418. Plaintiff Kachakech (for the purposes of this count, "Plaintiff") realleges and incorporates by reference the allegations contained in paragraphs 1 through 211 above, as if fully set forth herein.

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

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

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass Members' Private Information, which was a

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

direct and proximate cause of the Data Breach;

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

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

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

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

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

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

421. MCNA's representations and omissions were material because they were likely to

deceive reasonable consumers about the adequacy of MCNA's data security and ability to protect the confidentiality of consumers' Private Information.

422. MCNA acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiff and New York Subclass Members' rights. MCNA's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

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

424. MCNA's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the New Yorkers affected by the Data Breach.

425. The above deceptive and unlawful practices and acts by MCNA caused substantial injury to Plaintiff and New York Subclass Members that they could not reasonably avoid.

426. Plaintiff and New York Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs.

## CLAIM ON BEHALF OF THE TEXAS SUBCLASS

### COUNT XIX
### TEXAS DECEPTIVE TRADE PRACTICES–CONSUMER PROTECTION ACT
### Texas Bus. & Com. Code §§ 17.41 *et seq.*

427. Plaintiff Acosta and Plaintiff Hughes (for the purposes of this count, "Plaintiffs") reallege and incorporate by reference the allegations contained in paragraphs 1 through 211 above, as if fully set forth herein.

428. Plaintiffs bring this claim on behalf of themselves and the Texas Subclass.

429. MCNA is a "person," as defined by the Texas Trade Practices–Consumer Protection Act ("DTPA"), Tex. Bus. & Com. Code § 17.45(3).

430. Plaintiffs and the Texas Subclass Members are "consumers," as defined by Tex. Bus. & Com. Code § 17.45(4).

431. MCNA advertised, offered, or sold goods or services in Texas and engaged in trade or commerce directly or indirectly affecting the people of Texas, as defined by Tex. Bus. & Com. Code § 17.45(6).

432. MCNA engaged in false, misleading, or deceptive acts and practices, in violation of Tex. Bus. & Com. Code § 17.46(b), including:

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

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

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

d. Failing to disclose information concerning goods or services which was known at the time of the transaction if such failure to disclose such information was

intended to induce the consumer into a transaction into which the consumer would not have entered had the information been disclosed.

433. MCNA's false, misleading, and deceptive acts and practices include:

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

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

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Texas Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; HIPAA, 45 C.F.R. § 164; and Texas' data security statute, Tex. Bus. & Com. Code § 521.052, which was a direct and proximate cause of the Data Breach;

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

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Texas Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; HIPAA, 45 C.F.R. § 164; and Texas' data security statute, Tex. Bus. & Com. Code § 521.052;

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

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Texas Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; HIPAA, 45 C.F.R. § 164; and Texas' data security statute, Tex. Bus. & Com. Code § 521.052.

434. MCNA intended to mislead Plaintiffs and Texas Subclass Members and induce them to rely on its misrepresentations and omissions.

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

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

437. MCNA had a duty to disclose the above facts due to the circumstances of this case, the sensitivity and extent of the Private Information in its possession, and the generally accepted professional standards. Such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiffs and Texas Subclass Members, and MCNA because consumers are

unable to fully protect their interests with regard to their data, and placed trust and confidence in MCNA. MCNA's duty to disclose also arose from its:

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

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

c. Incomplete representations about the security and integrity of its computer and data systems, while purposefully withholding material facts from Plaintiffs and Texas Subclass Members that contradicted these representations.

438. MCNA engaged in unconscionable actions or courses of conduct, in violation of Tex. Bus. & Com. Code Ann. § 17.50(a)(3). MCNA engaged in acts or practices which, to consumers' detriment, took advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree.

439. Consumers, including Plaintiffs and Texas Subclass Members, lacked knowledge about deficiencies in MCNA's data security because this information was known exclusively by MCNA. Consumers also lacked the ability, experience, or capacity to secure the Private Information in MCNA's possession or to fully protect their interests with regard to their data. Plaintiffs and Texas Subclass Members lack expertise in information security matters and do not have access to MCNA's systems in order to evaluate its security controls. MCNA took advantage of its special skill and access to Private Information to hide its inability to protect the security and confidentiality of Plaintiffs' and Texas Subclass Members' Private Information.

440. MCNA intended to take advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree, with reckless disregard of the unfairness that would result. The unfairness resulting from MCNA's conduct is glaringly noticeable, flagrant,

complete, and unmitigated. The Data Breach, which resulted from MCNA's unconscionable business acts and practices, exposed Plaintiffs and Texas Subclass Members to a wholly unwarranted risk to the safety of their Private Information and the security of their identity or credit, and worked a substantial hardship on a significant and unprecedented number of consumers. Plaintiffs and Texas Subclass Members cannot mitigate this unfairness because they cannot undo the Data Breach.

441. MCNA acted intentionally, knowingly, and maliciously to violate Texas' Deceptive Trade Practices–Consumer Protection Act, and recklessly disregarded Plaintiffs' and Texas Subclass Members' rights.

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

443. MCNA's violations present a continuing risk to Plaintiffs and Texas Subclass Members, as well as to the general public.

444. On November 13, 2023, counsel for Plaintiffs provided written notice via certified mail to MCNA of the intent to pursue claims under the DTPA and an opportunity for MCNA to

cure. Plaintiffs' written notice set forth the violations of MCNA's duty to implement and maintain reasonable security procedures and practices alleged in this Complaint.

445. Contemporaneous with the filing of this Complaint, pursuant to Tex. Bus. & Com. Code Ann. § 17.501, Plaintiffs' counsel will send to the Consumer Protection Division a copy of the written notice sent to MCNA.

446. Plaintiffs and Texas Subclass Members seek damages, including economic damages, damages for mental anguish, statutory damages in the amount of three times the economic and mental anguish damages, as MCNA's acts were committed intentionally or knowingly, injunctive relief, other equitable relief the Court deems proper, costs, and reasonable and necessary attorneys' fees.

## CLAIM ON BEHALF OF THE UTAH SUBCLASS

### COUNT XX
### UTAH CONSUMER SALES PRACTICES ACT
### Utah Code §§ 13-11-1 *et seq.*

447. Plaintiff Hathaway (for the purposes of this count, "Plaintiff") realleges and incorporates by reference the allegations contained in paragraphs 1 through 211 above, as if fully set forth herein.

448. Plaintiff brings this claim on behalf of herself and the Utah Subclass.

449. MCNA is a "person" as defined by Utah Code § 13-11-3(5).

450. MCNA is a "supplier" as defined by Utah Code § 13-11-3(6) because it regularly solicits, engages in, or enforces consumer transactions, whether or not it deals directly with the consumer.

451. MCNA engaged in deceptive and unconscionable acts and practices in connection with consumer transactions, in violation of Utah Code §§ 13-11-4 and 13-11-5, including:

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

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

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Utah Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; HIPAA, 45 C.F.R. § 164; and the Utah Protection of Personal Information Act, Utah Code § 13-44-201, which was a direct and proximate cause of the Data Breach;

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

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Utah Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; HIPAA, 45 C.F.R. § 164; and the Utah Protection of Personal Information Act, Utah Code § 13-44-201;

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

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

Plaintiff's and Utah Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; HIPAA, 45 C.F.R. § 164; and the Utah Protection of Personal Information Act, Utah Code § 13-44-201.

452. MCNA's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of MCNA's data security and ability to protect the confidentiality of consumers' personal financial information.

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

454. MCNA's conduct was not only deceptive, but also unfair within the meaning of because it constitutes immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or competition. The injuries suffered by Plaintiff and the Utah Subclass are not outweighed by any countervailing benefits to consumers or competition. Because MCNA is solely responsible for securing its networks and protecting Private Information, there is no way Plaintiff and Utah Subclass Members could have known about MCNA's inadequate data security practices or avoided the injuries they sustained. There were reasonably available alternatives to further MCNA's legitimate business interests, other than its conduct responsible for the Data Breach.

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

of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

456. Plaintiff and Utah Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages; statutory damages of $2,000 per violation; amounts necessary to avoid unjust enrichment under Utah Code §§ 13-11-19 *et seq.*; injunctive relief; reasonable attorneys' fees and costs; and any other relief that is just and proper.

**PRAYER FOR RELIEF**

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

A. An order certifying this action as a class action and appointing Plaintiffs as Class representatives and the undersigned as Class Counsel;

B. A declaration that MCNA breached its duties to Plaintiffs and Class Members;

C. A mandatory injunction directing MCNA to adequately safeguard the Private Information of Plaintiffs and the Class hereinafter by implementing improved security procedures and measures;

D. A mandatory injunction requiring that MCNA provide notice to each Class Member relating to the full nature and extent of the Data Breach and the disclosure of Private Information to unauthorized persons;

E. An order enjoining MCNA from further unfair, deceptive, and unconscionable practices and making untrue statements about the Data Breach and the stolen Private Information;

F. An award of damages, including actual, nominal, consequential damages, statutory, and/or punitive, as allowed by law in an amount to be determined;

G. An award of pre- and post-judgment interest, costs, attorneys' fees, expenses, and

interest as permitted by law;

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

I. Such other and further relief as this court may deem just and proper.

## I. JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury for all issues so triable as of right.

Dated: November 13, 2023.

Respectfully Submitted,

By: *Stephanie A. Casey*
Stephanie A. Casey FBN 97483
**COLSON HICKS EIDSON, P.A.**
255 Alhambra Circle, Penthouse
Coral Gables, Florida 33134
Telephone: (305) 476-7400
scasey@colson.com

*Liaison Counsel for Plaintiffs and the Putative Classes*

Jeff Ostrow FBN 121452
**KOPELOWITZ OSTROW FERGUSON WEISELBERG GILBERT**
One West Las Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Telephone: (954) 332-4200
ostrow@kolawyers.com

Peter Prieto FBN 501492
**PODHURST ORSECK, P.A.**
One S.E. 3rd Avenue, Suite 2300
Miami, Florida 33131
Telephone: (305) 358-2800
pprieto@podhurst.com

*Interim Co-Lead Counsel for Plaintiffs and the Putative Classes*

mcnadental

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

To Enroll, Please Call:
1-888-220-5006
Or Visit:
https://response.idx.us/MCNA-Information
Enrollment Code: 7SAG5ZT86W

*40065226008207540 2*
000 0008573 00000000 0001 0004 02144 INS: 0 0

ALICIAH K SOUZA
10714 RITCHIE ST
BASTROP LA 71220-1869

54
14644

May 26, 2023

Su información personal puede haber estado involucrada en un incidente de datos. Si desea recibir una version de esta carta en español, por favor llame 1-888-220-5006.

**Notice of Data Breach**

Dear Aliciah K Souza:

We are sorry to tell you about a privacy event. This letter is from MCNA. We work with the Louisiana Department of Health; and the Children's Health Insurance Program to help provide benefits. This event may have involved your information.

**What happened?**
On March 6, 2023, MCNA became aware of certain activity in our computer system that happened without our permission. We quickly took steps to stop that activity. We began an investigation right away. A special team was hired to help us. We learned a cybercriminal was able to see and take copies of some information in our computer system between February 26, 2023 and March 7, 2023.

**What information may have been involved?**
On May 4, 2023, we told the state Medicaid agency that this event may have involved your information. Here is the kind of information that was seen and taken:

- Information used to contact you, like first and last name, address, date of birth, phone number, email
- Social Security number
- Driver's license number/other government-issued ID number
- Health insurance (plan information, insurance company, member number, Medicaid-Medicare ID numbers)
- Care for teeth or braces (visits, dentist name, doctor name, past care, x-rays/photos, medicines, and treatment)
- Bills and insurance claims

Some of this information was for a parent, guardian, or guarantor. A guarantor is the person who paid the bill. Information which was seen and taken was not the same for everyone.

**Why did this happen?**
A cybercriminal accessed our computer system without our permission.

**What was done about it?**
When we learned about the activity, we immediately began an investigation. Law enforcement was contacted. We are also making our computer systems even stronger than before because we do not want this to happen again.

We would like to offer you a free identity theft protection service. We will pay for the cost of this service for 1 year so that it is free for you. We have attached steps on how to sign up for this free service.

**Reference Guide**
**Review Your Account Statements**

Carefully review statements sent to you from your healthcare providers, insurance company, and financial institutions to ensure that all of your account activity is valid. Report any questionable charges promptly to the provider or company with which you maintain the account.

**Provide Any Updated Personal Information to Your Health Care Provider**

Your health care provider's office may ask to see a photo ID to verify your identity. Please bring a photo ID with you to every appointment if possible. Your provider's office may also ask you to confirm your date of birth, address, telephone, and other pertinent information so that they can make sure that all of your information is up-to-date. Please be sure and tell your provider's office when there are any changes to your information. Carefully reviewing this information with your provider's office at each visit can help to avoid problems and to address them quickly should there be any discrepancies.

**Order Your Free Credit Report**

To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

Upon receiving your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case. Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

**How to Enroll in IDX Credit and Identity Monitoring Services**

As a safeguard, you may enroll, at no cost to you, in an online credit monitoring and identity restoration service provided by IDX. To enroll in this service, please call 1-888-220-5006 or visit https://response.idx.us/MCNA-Information and follow the instructions for enrollment using the Enrollment Code provided above.

The monitoring included in the membership must be activated to be effective. You have until September 5, 2023 to enroll in these services. Please note that credit monitoring services may not be available for individuals who have not established credit or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score. If you need assistance, IDX will be able to assist you.

We encourage you to take advantage of these protections and remain vigilant for incidents of potential fraud and identity theft, including regularly reviewing and monitoring your credit reports and account statements.

**Contact the U.S. Federal Trade Commission**

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidents of identity theft or fraud, promptly report the matter to your local law enforcement authorities, state Attorney General and the FTC.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

**For Residents of Maryland**

You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, http://www.marylandattorneygeneral.gov/.

**For Residents of Massachusetts**

You have the right to obtain a police report with respect to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

**For Residents of New Mexico**

New Mexico consumers have the right to obtain a security freeze or submit a declaration of removal.

You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

(1) the unique personal identification number, password or similar device provided by the consumer reporting agency;

(2) proper identification to verify your identity; and

(3) information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

**For Residents of New York**

You may also obtain information about security breach response and identity theft prevention and protection from the New York Attorney General's Office:

Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, www.ag.ny.gov.

ATTENTION: If you speak English, language assistance services, free of charge, are available to you. Call 1-888-220-5006 (TTY: 1-888-220-5006).

ATENCIÓN: si habla español, tiene a su disposición servicios gratuitos de asistencia lingüística. Llame al 1-888-220-5006 (TTY: 1-888-220-5006).

ATANSYON: Si w pale Kreyòl Ayisyen, gen sèvis èd pou lang ki disponib gratis pou ou. Rele 1-888-220-5006 (TTY: 1-888-220-5006)

CHÚ Ý: Nếu bạn nói Tiếng Việt, có các dịch vụ hỗ trợ ngôn ngữ miễn phí dành cho bạn. Gọi số 11-888-220-5006 (TTY: 1-888-220-5006).

ATENÇÃO: Se fala português, encontram-se disponíveis serviços linguísticos, grátis. Ligue para 1-888-220-5006 (TTY: 1-888-220-5006).

注意:如果您使用繁體中文，您可以免費獲得語言援助服務。請致電1-888-220-5006 (TTY: 1-888-220-5006)。

ATTENTION : Si vous parlez français, des services d'aide linguistique vous sont proposés gratuitement. Appelez le 1-888-220-5006 (ATS : 1-888-220-5006).

PAUNAWA: Kung nagsasalita ka ng Tagalog, maaari kang gumamit ng mga serbisyo ng tulong sa wika nang walang bayad. Tumawag sa 1-888-220-5006 (TTY: 1-888-220-5006).

ВНИМАНИЕ: Если вы говорите на русском языке, то вам доступны бесплатные услуги перевода. Звоните 1-888-220-5006 (телетайп: 1-888-220-5006).

ملحوظة: إذا كنت تتحدث اذكر اللغة، فإن خدمات المساعدة اللغوية تتوافر لك بالمجان. اتصل برقم 1-888-220-5006 (رقم هاتف الصم والبكم: 1-888-220-5006).

ATTENZIONE: In cask la lingua palatal said litigant, so no disponibili servizi di assistenza linguistica gratuiti. Chiamare il numero 1-888-220-5006 (TTY: 1-888-220-5006).

ACHTUNG: Wenn Sie Deutsch sprechen, stehen Ihnen kostenlos sprachliche Hilfsdienstleistungen zur Verfügung. Rufnummer: 1-888-220-5006 (TTY: 1-888-220-5006).

주의: 한국어를 사용하시는 경우, 언어 지원 서비스를 무료로 이용하실 수 있습니다. 1-888-220-5006 (TTY: 1-888-220-5006)번으로 전화해 주십시오.

UWAGA: Jeżeli mówisz po polsku, możesz skorzystać z bezpłatnej pomocy językowej. Zadzwoń pod numer 1-888-220-5006 (TTY: 1-888-220-5006).

**સુચના: જો તમે ગુજરાતી બોલતા હો, તો નિ:શુલ્ક ભાષા સહાય સેવાઓ તમારા માટે ઉપલબ્ધ છે. ફોન કરો** 1-888-220-5006 (TTY: 1-888-220-5006).

เรียน :ถา้ คุณพดู ภาษาไทยคุณสามารถใชบ้ ริการช่วยเหลือทางภาษาไดฟ้ รี โทร 1-888-220-5006 (TTY: 1-888-220-5006).