IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

CYNTHIA WEISENBERGER, individually and on behalf of all others similarly situated, Plaintiff, v. AMERITAS MUTUAL HOLDING COMPANY, Defendant.	)	**Case No.** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Cynthia Weisenberger ("Plaintiff"), individually and on behalf of all others similarly situated, through the undersigned counsel, hereby allege the following against defendant Ameritas Mutual Holding Company ("Ameritas" or "Defendant"). Based upon personal knowledge as well as information and belief, Plaintiff specifically alleges as follows:

NATURE OF THE ACTION

1. This is a class action for damages with respect to Ameritas Mutual Holding Company, for its failure to exercise reasonable care in securing and safeguarding their customers' sensitive personal data— including names, addresses, email addresses, dates of birth, Social Security numbers, member ID numbers, policyholder names, employer names, and policy numbers, collectively known as personally identifiable information ("PII").

2. This class action is brought on behalf of customers whose sensitive PII was stolen by cybercriminals in a cyber-attack that accessed customer date through Ameritas's services on or around May 1 – June 4, 2019 (the "Data Breach").

3. The Data Breach affected at least 39,675 individuals from Ameritas services.

4. Ameritas reported to Plaintiff information compromised in the Data Breach included her PII.

5. Plaintiff was not notified until August 13, 2019, three months after her information was first accessed.

6. As a result of the Data Breach, Plaintiff has experienced various types of misuse regarding her PII over a two-year period, including unauthorized credit card charges, unauthorized access to her email accounts, fraudulent four credit cards closed over a period of two years, and consistent spam emails.

7. Plaintiff has mitigated harm by reporting the theft to the police, and filed an FTC fraud report that reported her identity theft to the FTC.

8. There has been no assurance offered from Ameritas that all personal data or copies of data has been recovered or destroyed. Ameritas offered Kroll credit monitoring, which does not guarantee security of Plaintiff's information. In order to mitigate further harm, Plaintiff chose not to disclose any more information to receive services connected with Ameritas.

9. Accordingly, Plaintiff asserts claims for violations of negligence, an intrusion upon seclusion, breach of implied contract, breach of fiduciary duty, breach of Nebraska Consumer Protection Act ("CPA"), Nebraska Revised Statutes § 59-1601, *et seq*., and a violation of the Nebraska Uniform Deceptive Trade Practices Act ("UDTPA"), Nebraska Revised Statutes §§ 87-301, *et. seq*.

PARTIES

Plaintiff Cynthia Weisenberger

10. Plaintiff Cynthia Weisenberger is a resident of North Carolina and brings this action in her individual capacity and on behalf of all others similarly situated. Weisenberger paid

Defendant over $40 a month over a period of at least three years to receive a dental insurance policy from Defendant. To receive the dental insurance policy, Defendant required her to disclose her PII, which it expressly and impliedly promised to safeguard. Defendant, however, did not take proper care of Weisenberger's PII, leading to its exposure as a result of Defendant's inadequate security. In April 2019, Weisenberger received a notification letter from Defendant stating her PII was taken, which included, "names, addresses, email addresses, dates of birth, Social Security numbers, member ID numbers, policyholder names, employer names, and policy numbers." The letter also advised Weisenberger to contact the Federal Trade Commission. In response to the recommendation, Weisenberger put a fraud alert on her information through the FTC. Additionally, Weisenberger reported the leak to her local police department. The police could not help her due to the high volume of data breach reports they consistently receive.

11. The letter also offered one year of credit monitoring through Kroll, which was ineffective for Weisenberger and Class members. The Kroll credit monitoring would have shared her information with third parties and could not guarantee complete privacy of her sensitive PII.

12. In the two years following the breach, Weisenberger experienced a slew of harms as a result of the data breach. She lost $280 due to fraudulent activity on her Amazon account that was not refunded, her bank had to replace her credit cards four times due to fraudulent charges, and two of her email accounts were compromised. She has also received targeted advertising for credit monitoring. To mitigate further harm, she's followed the Federal Trade Commission's advice and put a fraud alert on her credit report.

Defendant

13. Defendant Ameritas Mutual Holding Company. is a Nebraska insurance company., which operates nationally, including in North Carolina. Ameritas offers multiple products, including

dental insurance. Ameritas is the marketing name for subsidiaries of Ameritas Mutual Holding Company including but not limited to, Ameritas Life Insurance Corp. Ameritas registered its headquarters at 5900 O Street, Lincoln, NE 68510.

14. Ameritas closed its 2019 revenue with $2.5 billion in total revenue, an 5% increase from their previous year.[1]

JURISDICTION AND VENUE

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

14. The Court has personal jurisdiction over Defendant because Defendant's principal place of business is located in this District.

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

FACTS

16. Defendant provides insurance to thousands of customers in North Carolina and across the country. As part of its business, Defendant stores a vast amount of its customers' Private Information. In doing so, Defendant was entrusted with, and obligated to safeguard and

[1] https://www.ameritas.com/OCM/GetPDF?pdfname=511305

protect, the Private Information of Plaintiff and the Class in accordance with all applicable laws.

17. In May of 2019, Defendant first learned of unauthorized entry into its network, which contained customers' Private Information including names, addresses, email addresses, dates of birth, Social Security numbers, member ID numbers, policyholder names, employer names, and policy numbers.

18. Upon learning of the Security Breach in May 2019, Defendant investigated. As a result of the Security Breach, Defendant initially estimated that the Private Information of 39,675 customers were potentially compromised stemming from services previously received.

19. In May 2019 Defendant announced that it first learned of suspicious activity that allowed one or more cybercriminals to access their systems through a phishing attack. The 2019 Notice disclosed that a phishing campaign enabled a threat actor to access Ameritas' systems.

20. Defendant offered no explanation for the delay between the initial discovery of the Breach and the belated notification to affected customers.

21. Defendant has yet to affirmatively notify impacted customers individually regarding which specific data of theirs were stolen, yet customers have already fallen victim to thieves using customers' exposed information.

22. The Breach occurred because Defendant failed to take reasonable measures to protect the Personal Identifiable Information it collected and stored. Among other things, Defendant failed to implement data security measures designed to prevent this attack, despite repeated warnings to the healthcare industry, insurance companies, and associated entities about the risk of cyberattacks and the highly publicized occurrence of many similar attacks in the recent past

on other healthcare providers.

Defendant Failed to Maintain Reasonable and Adequate Security Measures to Safeguard Customers' Private Information

23. Defendant failed to properly safeguard Class members' Private Information, allowing hackers to access their Private Information.

24. Defendant had obligations created by industry standards, common law, and representations made to Class members, to keep Class members' Private Information confidential and to protect it from unauthorized access and disclosure.

25. Plaintiff and Class members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant and any of its affiliates would comply with their obligations to keep such information confidential and secure from unauthorized access.

26. Prior to and during the Security Breach, Defendant promised customers that their Private Information would be kept confidential.

27. Defendant's failure to provide adequate security measures to safeguard customers' Private Information is especially egregious because Defendant operates in a field which has recently been a frequent target of scammers attempting to fraudulently gain access to customers' highly confidential Private Information.

28. In fact, Defendant has been on notice for years that the medical industry and its associated insurance companies are a prime target for scammers because of the amount of confidential customer information maintained. In 2019 alone, numerous entities in the healthcare sector suffered high-profile data breaches including Quest Diagnostics and Lab

Corp. Prior to 2019 high-profile breaches like Equifax and Yahoo warned all companies of the risks.

Damages to Plaintiff and the Class

29. Plaintiff and the Class have been damaged by the compromise of their Private Information in the Security Breach.

30. Plaintiff and the Class have suffered or face a substantial risk of suffering out-of-pocket fraud losses such as fraudulent charges on online accounts, credit card fraud, loans opened in their names, medical services billed in their name, and similar identity theft.

31. Class members have or may have incurred out of pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Security Breach.

32. While Defendant offered one year of credit monitoring, Plaintiff could not trust a company that had already breached her data. The credit monitoring offered from Kroll does not guarantee privacy or data security for Plaintiff who would have to expose her information once more to get monitoring services. Thus, to mitigate harm, Plaintiff and Class members are now burdened with indefinite monitoring and vigilance of their accounts. For example, Plaintiff caught $280 of fraud charged to her Amazon account because she was vigilant, but despite her vigilance, she was not reimbursed for her loss from the fraud.

33. Plaintiff and Class members suffered a "loss of value" of their Private Information when it was acquired by cyber thieves in the Security Breach. Plaintiff has already experienced had her information taken and used fraudulently online.

34. Class members who paid Defendant for their services overpaid for a service that was intended to be accompanied by adequate data security, but was not. Part of the price Class

members paid to Defendant was intended to be used by Defendant to fund adequate data security. Defendant did not properly comply with their data security obligations. Thus, the Class members did not get what they paid for.

35. Plaintiff would not have obtained services from Defendant had Defendant told her that it failed to maintain adequate computer systems and data security practices to safeguard her Private Information from theft.

36. Members of the Class will continue to spend significant amounts of time to monitor their financial and medical accounts for misuse.

37. According to the U.S. Department of Justice Bureau of Justice Statistics, an estimated 17.6 million people were victims of one or more incidents of identity theft in 2014. Among identity theft victims, existing bank or credit accounts were the most common types of misused information.[2]

38. Similarly, the FTC cautions that identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[3]

39. The theft of Social Security Numbers, which were purloined as part of the Security Breach, is particularly detrimental to victims. The U.S. Social Security Administration (SSA)

[2] *See* DOJ, *Victims of Identity Theft, 2014* at 1 (Nov. 13, 2017), available at https://www.bjs.gov/content/pub/pdf/vit14.pdf.

[3] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number[.]" *Id.*

warns that "[i]dentity theft is one of the fastest growing crimes in America."[4] The SSA has stated that "[i]dentity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought." *Id.* In short, "[s]omeone illegally using your Social Security number and assuming your identity can cause a lot of problems." *Id.*

40. In fact, a new Social Security number is substantially less effective where "other personal information, such as [the victim's] name and address, remains the same" and for some victims, "a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under your new number may make it more difficult for you to get credit." *Id.*

41. Identity thieves can use the victim's Private Information to commit any number of frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest. In the insurance context, Private Information can be used to submit false insurance claims. As a result, Plaintiff and Class members now face a real and continuing immediate risk of identity theft and other problems associated with the disclosure of their Social Security numbers, and will need to monitor their credit for an indefinite duration. For Plaintiff and Class members, this risk creates unending feelings of fear and annoyance.

42. Private information is especially valuable to identity thieves. Defendant knew or should have known this and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare

[4] Identity Theft And Your Social Security Number, Social Security Administration (Dec. 2013), http://www.ssa.gov/pubs/EN-05-10064.pdf.

for that risk.

The Monetary Value of Privacy Protections and Private Information

43. The fact that Plaintiff's and Class members' Private Information was stolen—and might presently be offered for sale to cyber criminals—demonstrates the monetary value of the Private Information.

44. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[5]

45. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States.[6]

46. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information

[5] Tr. at 8:2-8, Federal Trade Commission, *Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data* (Mar. 13, 2001) available at https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

[6] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal (Feb. 28, 2011), http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html.

> may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[7]

47. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information.[8] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

48. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349.[9]

49. The value of Plaintiff' and Class members' Private Information on the black market is substantial, ranging, for example, from $1.50 to $90 per payment card number.[10]

50. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the Private Information it maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud. Defendant should have particularly been aware of these risks given the significant number of data breaches affecting the medical industry and related industries.

[7] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.
[8] *Web's Hot New Commodity: Privacy*, *supra* note 7.
[9] *See* DOJ, *Victims of Identity Theft, 2014*, *supra* note 3, at 6.

[10] Leapfrog, *The Cyber Black Market: What's Your Bank Login Worth* (Mar. 1, 2011), available at https://leapfrogservices.com/the-cyber-black-market-whats-your-bank-login-worth/.

51. Had Defendant remedied the deficiencies in its security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Defendant would have prevented the phishing attack into their systems and, ultimately, the theft of their customers' Private Information.

52. Given these facts, any company that transacts business with customers and then compromises the privacy of customers' Private Information has thus deprived customers of the full monetary value of their transaction with the company.

53. Acknowledging the damage to Plaintiff and Class members, Defendant instructed customers like Plaintiff to "regularly review the statements that you receive from your healthcare insurers and providers. If you identify services that you did not receive, please contact the insurer or provider immediately." Plaintiff and the other Class members now face a greater risk of identity theft

CLASS ACTION ALLEGATIONS

54. Plaintiff incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

55. Plaintiff brings this action individually and on behalf of all other persons similarly situated ("the Class") pursuant to Federal Rule of Civil Procedure 23.

56. Plaintiff proposes the following Class definition subject to amendment based on information obtained through discovery. Notwithstanding, at this time, Plaintiff brings this action and seeks certification of the following Class:

> All persons whose Private Information was compromised as a result of the Security Breach discovered on or about May 2019 and who were sent notice of the Security Breach.

Excluded from the Class are Defendant and Defendant's affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

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

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

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

a. Whether Defendant's data security systems prior to and during the Security Breach complied with applicable data security laws and regulations;

b. Whether Defendant's data security systems prior to and during the Security Breach were consistent with industry standards;

c. Whether Defendant properly implemented its purported security measures to protect Plaintiff's and the Class's Private Information from unauthorized capture, dissemination, and misuse;

d. Whether Defendant took reasonable measures to determine the extent of the Security Breach after it first learned of same;

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

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

g. Whether Defendant was negligent in failing to properly secure and protect Plaintiff's and the Class's Private Information;

h. Whether Defendant was unjustly enriched by its actions; and

i. Whether Plaintiff and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

60. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and other members of the Class. Similar or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

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

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

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

64. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the other members of the Class are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for members of the Class to individually seek redress for Defendant's wrongful conduct. Even if members of the Class could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and All Class Members)

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

66. Upon Defendant's accepting and storing the Private Information of Plaintiff and the Class in their computer systems and on their networks, Defendant undertook and owed a duty to Plaintiff and the Class to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendant knew that the Private Information was private and confidential and should be protected as private and confidential.

67. Defendant owed a duty of care not to subject Plaintiff's and the Class's Private Information to an unreasonable risk of exposure and theft because Plaintiff and the Class were foreseeable and probable victims of any inadequate security practices.

68. Defendant owed numerous duties to Plaintiff and the Class, including the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information in their possession;
b. to protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and
c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

69. Defendant also breached their duty to Plaintiff and Class members to adequately protect and safeguard Private Information by disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information. Furthering their dilatory practices, Defendant failed to provide adequate supervision and oversight of the Private Information with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a malicious

third party to gather Plaintiff's and Class members' Private Information and potentially misuse the Private Information and intentionally disclose it to others without consent.

70. Defendant knew, or should have known, of the risks inherent in collecting and storing Private Information and the importance of adequate security. Defendant knew or should have known about numerous well-publicized data breaches within the medical industry.

71. Defendant knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiff's and Class members' Private Information.

72. Defendant breached their duties to Plaintiff and Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and Class members' Private Information.

73. Because Defendant knew that a breach of their systems would damage thousands of their customers, including Plaintiff and Class members, Defendant had a duty to adequately protect their data systems and the Private Information contained thereon.

74. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its customers, which is recognized by laws and regulations including but not limited to common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class members from a data breach.

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

76. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant are bound by industry standards to protect confidential Private Information.

77. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their Private Information. Defendant's misconduct included failing to: (1) secure Plaintiff's and Class member's Private Information; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

78. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class members' Private Information, and by failing to provide timely notice of the Security Breach. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

1. Failing to adopt, implement, and maintain adequate security measures to safeguard Class members' Private Information;
2. Failing to adequately monitor the security of Defendant's networks and systems;
3. Allowing unauthorized access to Class members' Private Information;
4. Failing to detect in a timely manner that Class members' Private Information had been compromised; and
5. Failing to timely notify Class members about the Security Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages

79. Through Defendant's acts and omissions described in this Complaint, including its failure to provide adequate security and failure to protect Plaintiff's and Class members' Private Information from being foreseeably captured, accessed, disseminated, stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff's and Class members' Private Information during the time it was within Defendant's possession or control.

80. Defendant's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to failing to adequately protect the Private Information and failing to provide Plaintiff and Class members with timely notice that their sensitive Private Information had been compromised.

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

82. As a direct and proximate cause of Defendant's conduct, Plaintiff and Class members suffered damages as alleged above.

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

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiff and All Class Members)

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

85. Through their course of conduct, Defendant, Plaintiff, and Class Members entered into implied contracts for the provision of insurance, as well as implied contracts for the Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

86. Specifically, Plaintiff entered into a valid and enforceable implied contract with Defendant when she first entered into insurance agreement with Defendant.

87. The valid and enforceable implied contracts to provide insurance services that Plaintiff and Class Members entered into with Defendant include Defendant's promise to protect nonpublic Private Information given to Defendant or that Defendant creates on its own from disclosure.

88. When Plaintiff and Class Members provided their Private Information to Defendant in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

89. Defendant solicited and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

90. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, and were consistent with industry standards.

91. Class members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

92. Under implied contracts, Defendant and/or its affiliated providers promised and were obligated to: (a) provide insurance to Plaintiff and Class Members; and (b) protect Plaintiff's and the Class Members' Private Information provided to obtain such benefits of insurance policy. In exchange, Plaintiff and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

93. Both the provision of insurance and the protection of Plaintiff's and Class Members' Private Information were material aspects of these implied contracts.

94. The implied contracts for the provision of insurance services – contracts that include the contractual obligations to maintain the privacy of Plaintiff's and Class Members' Private Information- are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendant's Security Breach notification letter.

95. Defendant's express representations, including, but not limited to the express representations found in its Privacy Notice, memorializes and embodies the implied contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and protect the privacy of Plaintiff's and Class members Private Information.

96. Consumers of insurance value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining insurance private. To customers such as Plaintiff and Class members, insurance that does not adhere to industry standard data security. Plaintiff and Class members would not have entrusted their Private Information to Defendant and entered into these implied contracts with Defendant without an understanding that their Private Information would be safeguarded and protected, or entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

97. A meeting of the minds occurred, as Plaintiff and Class members agreed and provided their Private Information to Defendant and/or its affiliated healthcare providers, and paid for the provided insurance in exchange for, amongst other things, both the provision of healthcare and insurance services and the protection of their Private Information.

98. Plaintiff and Class members performed their obligations under the contract when they paid for Defendant's services and provided their Private Information.

99. Defendant materially breached its contractual obligation to protect the nonpublic Private Information Defendant gathered when the information was accessed and exfiltrated by the Security Breach.

100. Defendant materially breached the terms of the implied contracts, including, but not limited to, the terms stated in the relevant Notice of Privacy Practices. Defendant did not maintain the privacy of Plaintiff's and Class members Private Information as evidenced by its notifications of the Security Breach to Plaintiff and Class members. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA, or otherwise protect Plaintiff's and Class members private information as set forth above.

101. The Security Breach was a reasonably foreseeable consequence of Defendant's action in breach of these contracts.

102. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiff and Class members did not receive full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts. Plaintiff and Class members therefore were damaged in an amount at least equal to the difference in the value of the healthcare with data security protection they paid for and the healthcare they received.

103. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiff, Class members, nor any reasonable person would have purchased healthcare from Defendant and/or its affiliated providers.

104. As a direct and proximate result of the Security Breach, Plaintiff and Class members have been harmed and suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out of pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

105. Plaintiff and Class members are entitled to compensatory and consequential damages suffered as a result of the Security Breach.

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

COUNT III
Breach of Fiduciary Duty
(On Behalf of Plaintiff and All Class Members)

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

108. In providing their Private Information to Defendant, Plaintiff and Class Members justifiably placed a special confidence in Defendant to act in good faith and with due regard to

interests of Plaintiff and Class members to safeguard and keep confidential that Private Information.

109. Defendant accepted the special confidence Plaintiff and Class members placed in it, as evidenced by its assertion that it "takes the protection and proper use of [Plaintiff's] information very seriously" as included in the Security Breach notification letter.

110. In light of the special relationship between Defendant and Plaintiff and Class members, whereby Defendant became a guardian of Plaintiff's and Class members Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its customers, including Plaintiff and Class members for the safeguarding of Plaintiff and Class member's Private Information.

111. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of its customer's relationship, in particular, to keep secure the Private Information of its customers.

112. Defendant breached its fiduciary duties to Plaintiff and Class members by failing to diligently discover, investigate, and give notice of the Security Breach effects in a reasonable and practicable period of time.

113. Defendant breached its fiduciary duties to Plaintiff and Class members by failing to protect the integrity of the systems containing Plaintiff's and Class member's Private Information.

114. Defendant breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

115. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i)

actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Cyber-Attack and data breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Cyber-Attack and data breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

116. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT IV

Breach of Nebraska Consumer Protection Act ("CPA"), Nebraska Revised Statutes § 59-1601, *et seq*.,

(On Behalf of Plaintiff and All Class Members)

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

118. Plaintiff, Class members, and Defendant each qualify as a person engaged in trade or commerce as contemplated by the Nebraska Consumer Protection Act ("CPA"), Neb. Rev. Stat. § 59-1601, et seq.

119. As alleged herein this Complaint, Defendant engaged in unfair or deceptive acts or practices in the conduct of consumer transactions in violation of the CPA, including but not limited to:

1. representing that its services were of a particular standard or quality that it knew or should have known were of another;

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

3. Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Security Breach;

4. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Cyber-Attack and data breach;

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

6. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' Private Information; and

7. 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 Class Members' Personal Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Security breach.

120. Defendant's representations and omissions were material because it was likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

121. In addition, Defendant's failure to secure consumers' PHI violated the FTCA and therefore violates the CPA.

122. Also, Defendant's failure to give timely notice of this Security Breach in violation Nebraska's notification of security breach statute, Neb. Rev. Stat. § 87-801 et seq is an unfair or deceptive act pursuant to Neb. Rev. Stat. § 87-808, and therefore violates the Consumer Protection Act.

123. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the PII of Plaintiff and Class Members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

124. The aforesaid conduct constitutes a violation of the CPA, Neb. Rev. Stat. § 59-1603, in that it is a restraint on trade or commerce.

125. These violations have caused financial injury to the Plaintiff

126. and the other Class Members.

127. The Defendant's violations of the CPA have an impact of great or general importance on the public.

128. As a direct and proximate result of Defendant's violation of the CPA, Plaintiff and Class Members are entitled to a judgment under Neb. Rev. Stat. § 59-1609 to enjoin further

violations, to recover actual damages, to recover the costs of this action (including reasonable attorney's fees), and such other further relief as the Court deems just and proper.

COUNT V
VIOLATION OF NEBRASKA UNIFORM DECEPTIVE TRADE PRACTICES ACT
Nebraska Revised Statutes § 87-301, et seq.
(On Behalf of Plaintiff and Class Members)

129. Plaintiff, all Class members and Defendant each qualify as a person engaged in trade or commerce as contemplated by the Nebraska Uniform Deceptive Trade Practices Act ("UDTPA"), Neb. Rev. Stat. § 87-301, et seq.

130. Defendant's implied and express representations that it would adequately safeguard Plaintiff's and Class members' Private Information constitute 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).

131. Defendant's implied and express representations that it would adequately safeguard Plaintiff's and Class members' Private Information constitute 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).

132. Defendant knowingly made false or misleading statements in its privacy policy regarding the use of personal information submitted by members of the public in that Defendant advertised it is "committed to protecting your privacy and securely maintaining your personal information." [11] Defendant did not securely maintain personal information as represented, in violation of Neb. Rev. Stat. § 87-302(a)(15).

[11] https://www.ameritas.com/about/privacy/

133. These violations have caused financial injury to Plaintiff and Class Members and have created an unreasonable, imminent risk of future injury.

134. Accordingly, Plaintiff, on behalf of herself and Class members, bring this action under the Uniform Deceptive Trade Practices Act to seek such injunctive relief necessary to enjoin further violations and to recover costs of this action, including reasonable attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Defendant, as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Classes;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from failing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Security Breach;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

E. Ordering Defendant to pay for not less than three (3) years of credit monitoring services for Plaintiff and the Classes;

F. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

G. For an award of punitive damages, as allowable by law;

H. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

I. Pre- and post-judgment interest on any amounts awarded; and

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

Date: August 17, 2021

Respectfully submitted,

Vincent M. Powers Bar No. 15866
POWERS LAW
411 South 13th Street, Suite 300
Lincoln, NE 68508
Tel: (402) 474-8000
powerslaw@me.com

Jason S. Rathod*
jrathod@classlawdc.com
Nicholas A. Migliaccio*
nmigliaccio@classlawdc.com
Migliaccio & Rathod LLP
412 H Street NE
Washington, DC 20002
Tel: (202) 470-3520
Fax: (202) 800-2730

*Permanently Admitted to Practice in D. Neb.