UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
FORT LAUDERDALE DIVISION

Taylor Manning on behalf of himself and all others similarly situated,

Plaintiff,

vs.

MANAGED CARE OF NORTH AMERICA, INC., dba MCNA DENTAL

Defendant.

/

CLASS ACTION

CASE NO:

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Taylor Manning ("Plaintiff"), individually and on behalf of all other persons similarly situated, by and through his attorneys, upon personal knowledge as to himself and his own acts and experiences, upon investigation of counsel, and upon information and belief as to all other matters, alleges as follows:

NATURE OF THE ACTION

1. Plaintiff brings this Class Action Complaint against Defendant Managed Care of North America, Inc., dba MCNA Dental ("MCNA" or "Defendant"), to hold Defendant accountable for the harm they caused to Plaintiff and nearly nine million similarly situated persons (including minors) ("Class Members"), from its failure to properly secure and safeguard current and former patients' sensitive personally identifiable information ("PII"), including their names, addresses, telephone numbers, email addresses, birth dates, Social Security numbers, driver's license numbers, government-issued ID numbers, health insurance information,

Medicare/Medicaid ID numbers, group plan names and numbers, and protected health information ("PHI") such as dental and orthodontic treatment.

2. The full extent of the types of sensitive personal information, the scope of the breach, and the root cause of the Data Breach is all within the exclusive control of Defendant and its agents, counsel, and forensic security vendors at this phase of litigation.

3. Plaintiff received a letter dated May 26, 2023, similar to a letter Defendant submitted to the Office of the Maine Attorney General.[1] The notice letter stated that on March 6, 2023, MCNA became aware that an unauthorized party was able to access certain MCNA systems and infect them with malicious code. Through a subsequent investigation, MCNA determined that the unauthorized third party was able to access and remove copies of PII and PHI between February 26, 2023, and March 7, 2023 (the "Data Breach").

4. LockBit ransomware group has claimed responsibility for the attack and leaked the stolen data on its dark web data leak site as proof of data theft. The first data samples from the Data Breach were published on the dark web on March 7, 2023. LockBit demanded a $10 million ransom to prevent the publication of all of the stolen data. Upon information and belief, the ransom was not paid, as the group published the stolen files on April 7, 2023.

5. The Data Breach occurred because Defendant failed to implement adequate, reasonable, and industry-mandated cyber-security procedures and protocols to protect the PII and PHI of Plaintiff and Class Members. Indeed, the deficiencies in Defendant's data security protocols and practices were so significant that unauthorized person(s) were able to access, view and remove or download patient data.

[1] *See Data Breach Notifications*, Me. Att'y. Gen., attached as Ex. 1.

6. Defendant did not adequately safeguard and protect Plaintiff's PII and PHI, and now Plaintiff, along with millions of other Class Members, is the victim of a significant Data Breach that, among other harms, puts Plaintiff at a substantially increased risk of identity fraud, which will negatively impact Plaintiff for years to come.

7. Defendant is responsible for this Data Breach through its failure to implement and maintain adequate and reasonable data security safeguards, its failure to comply with industry-standard data security practices, and its failure to comply with federal and state laws and regulations governing data security and privacy of PII and PHI.

8. Despite its role in managing so much sensitive and personal PII and PHI, Defendant failed to timely recognize and detect the unauthorized access and use of its systems, and further failed to timely recognize that substantial amounts of data had been compromised.

9. Defendant failed to, among other things, timely detect that a criminal third party had accessed its computer systems, failed to notice that massive amounts of data were compromised, and failed to take any steps to investigate red flags that should have warned Defendant that its systems were not secure and were being targeted and attacked. Had Defendant properly maintained and monitored its information technology infrastructure and denied or circumvented access to that infrastructure to all potential and active threats, Defendant would have discovered the invasion sooner – and/or prevented it altogether.

10. Defendant had numerous statutory, regulatory, and common law duties to Plaintiff and Class Members to keep their PII, including PHI, confidential, safe, secure, and protected from unauthorized disclosure or access, including duties under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Defendant was and is still required to maintain the security and privacy of the PII and PHI entrusted to it. When Plaintiff and Class Members provided

their PII and PHI, Defendant and its agents were required to comply with these obligations to keep Plaintiff's PII and PHI secure and safe from unauthorized access, to use this information for business purposes only, and to make only authorized disclosures of this information.

11. In this era of frequent data security attacks and data breaches, particularly in the healthcare industry, Defendant's failures leading to the Data Breach are particularly egregious.

12. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI.

13. As a result of Defendant's failures, the PII and PHI of Plaintiff and Class Members were accessed and downloaded by one or more malicious actors. As a direct and proximate result, Plaintiff and Class Members are now at a significant present and future risk of identity theft, financial fraud, and/or other identity-theft or fraud, imminently and for years to come.

14. Plaintiff's and Class Members' injuries described herein were exacerbated by the delay in informing and notifying Plaintiff and Class Members of the Data Breach and the theft of their PII and PHI. Plaintiff and Class Members were unable to take actions to protect themselves and attempt to mitigate the harm until they received notice.

15. Plaintiff and Class Members have suffered numerous actual and imminent injuries as a direct result of the Data Breach, including: (a) theft of their valuable PII and PHI; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of the Data Breach; (d) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft posed by their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (e) damages to and diminution in value of their personal data; (f) invasion of privacy; (g) actual damages in the form of the difference in

value between the services that should have been delivered and the services that were actually delivered; and (h) the continued risk to their PII and PHI, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII and PHI.

16. Plaintiff seeks to remedy these harms, and to prevent their future occurrence, on behalf of Plaintiff and all similarly situated persons whose PII and PHI were compromised as a result of the Data Breach.

17. Accordingly, Plaintiff, on behalf of himself and Class Members, asserts claims for negligence, breach of implied contract and unjust enrichment. Plaintiff seeks all relief as authorized in equity or by law.

THE PARTIES

Defendant

18. Defendant MCNA is a Florida corporation with its principal place of business in Fort Lauderdale, Florida.

19. MCNA is the largest dental insurer in the nation for government-sponsored Medicaid and Children's Health Insurance Programs ("CHIP"). MCNA has been in business for nearly thirty years and is dedicated to promoting "high-quality and cost-effective oral health by increasing access to dental care for the public.[2]" Together with its affiliates, MCNA claims to provide "exceptional service" to state agencies and managed care organizations all across the nation.[3]

20. On its website, MCNA touts that it's services and programs are "built to meet and

[2] https://www.mcna.net/en/home (last visited June 8, 2023).
[3] See *id.*

exceed industry standards and best practices.[4]"

Plaintiff

21. Plaintiff Taylor Manning is a citizen of Louisiana.

22. Plaintiff is very careful about sharing his PII and PHI and has never knowingly transmitted his PII and PHI unencrypted over the internet or any other unsecured source. Plaintiff stores all documents containing his PII and PHI in a safe and secure location and destroys any documents he receives in the mail that may contain any information that could be used to compromise his financial accounts, commit fraud, and steal his identity.

23. Plaintiff has sought treatment for dental care and has seen dentists related to those issues over the years. He provided those providers with his PII and PHI in order to receive treatment services prior to the Data Breach.

24. Plaintiff received Defendant's Notice of Data Breach on or about June 12, 2023. The notice informed Plaintiff that Defendant's systems had been compromised and that Plaintiff's name and contact information, his Social Security number, driver's license number, health insurance information, and treatment information may have been "seen and taken."

25. Upon information and belief, Plaintiff's PII and PHI was targeted, accessed, and downloaded by the third party criminal actors in the Data Breach.

26. Upon information and belief, Plaintiff's PII and PHI was published on the dark web following the Data Breach.

27. As a result of the Data Breach, Plaintiff forever faces a substantial risk of imminent identity, financial, and health fraud and theft.

28. In response to the Data Breach and fraudulent activity, Plaintiff made reasonable

[4] See *id.*

efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; researching credit monitoring and identity theft protection services. This is valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work, recreation, and the private enjoyment of life.

29. Plaintiff is deeply concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

JURISDICTION & VENUE

30. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. §1332(d)(2), because this is a putative class action involving more than 100 Class Members and because the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Moreover, Plaintiff, many absent Class Members, and Defendant are citizens of different states.

31. This Court has general personal jurisdiction over Defendant because its principal place of business is located in this district.

32. Venue is proper in this district under 28 U.S.C. §§1391(a)(1), 1391(b)(1), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this district, Defendant conducts substantial business in this district, and Defendant resides in this district. On information and belief, Plaintiff's and Class Members' PII and PHI was transmitted to and by Defendant and input into their network within the district. Defendant is based in this district, are believed to maintain Plaintiff's and Class Members' PII and PHI in the district and the harm caused to Plaintiff and Class Members emanated from this district.

FACTUAL ALLEGATIONS

Defendant Acquires, Collects, and Maintains Plaintiff's and Class Members' PII and PHI.

33. Insurers, individuals, private employers, and families contract with Defendant to

provide an allegedly more efficient process by which patient claims may be processed.

34. In connection with procuring and providing dental services to patients such as Plaintiff and Class Members, MCNA acquires, collects, and maintains a massive amount of PHI and other PII of patients.

35. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and the Class Members' PII and PHI, Defendant assumed legal and equitable duties to those individuals and knew or should have known that they were responsible for protecting Plaintiff's and Class Members' PII and PHI from disclosure.

36. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI. Defendant was required to keep Plaintiff's and Class Members' PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

The Data Breach

37. Defendant provided notice to various state Attorneys General of a Data Breach it experienced, including the Maine Attorney General. Defendant provided the Maine Attorney General with a template of a letter it was providing to affected individuals. The template letter states, in part:

> **What Happened?**
>
> On March 6, 2023, MCNA became aware that an unauthorized party was able to access certain MCNA systems. Upon discovery the same day, MCNA took immediate steps to contain the threat and engaged a third-party forensic firm to investigate the incident and assist with remediation efforts. 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. MCNA undertook an extensive review to determine what data may have been impacted. As a result of this review, which was completed on May 3, 2023, it appears that your personal information may have been involved.

> **What information was involved?**
>
> Personal information that may have been involved included: (1) demographic information to identify and contact you, such as full name, date of birth, address, telephone and email; (2) Social Security number; (3) driver's license number or government-issued identification number; (4) health insurance information, such as name of plan/insurer/government payor, member/Medicaid/Medicare ID number, plan and/or group number; and (5) information regarding dental/orthodontic care. Not all data elements were involved for all individuals.[5]

38. The template letter directed Plaintiff and Class Members to "carefully review credit reports and statements sent from providers as well as [their] insurance company[.]"

39. Defendant began notifying the individual victims of the Data Breach in late May 2023. Plaintiff received a Data Breach notice letters Defendant dated May 28, 2023, notifying him of the Data Breach. The letter is substantially the same as the template letter.

40. The Data Breach notice Plaintiff received offered him one year of credit monitoring services. This is wholly inadequate because victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft. Moreover, Defendant's offer does not address any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII and PHI, including private and sensitive medical information.

41. Furthermore, Defendant's providing information on how to sign up for free credit monitoring squarely places the burden on Plaintiff and Class Members, rather than Defendant, to investigate and protect themselves from Defendant's tortious acts resulting in the Data Breach. Rather than automatically enrolling Plaintiff and Class Members in credit monitoring services upon discovery of the Data Breach, Defendant merely sent instructions offering the services to affected patients recommending they sign up for the services.

42. Based on Defendant's urging Plaintiff and Class Members to take mitigating

[5] Me. Att'y Gen. Notice, Ex. 1.

actions, it is abundantly clear that the perils from the Data Breach are real and concrete, and not hypothetical or attenuated.

43. Despite all of the publicly available knowledge of the continued compromises of PII and PHI, Defendant's approach to maintaining the privacy of Plaintiff's and Class Members' PII and PHI was inadequate, unreasonable, reckless, and negligent. This is evidenced by Defendant's Data Breach notice, wherein Defendant stated in response to the Data Breach that they are "making [their] computer systems even stronger than before." Implied in Defendant's statement is an admission that Defendant's technical and cybersecurity capabilities were inadequate, which resulted in the Data Breach and the divulgence of Plaintiff's and Class Members' PII and PHI.

Defendant Knew It Was, and Continues to Be, a Prime Target for Cyberattacks.

44. Defendant is fully aware of how sensitive the PII and PHI it stores and maintains is. It is also aware of how much PII and PHI it collects, use, and maintains from Plaintiff and Class Members.

45. Businesses that store personal information are likely to be targeted by cyber criminals. Credit card and bank account numbers are tempting targets for hackers, but credit and debit cards can be cancelled, quickly mitigating the hackers' ability to cause further harm. Instead, PHI and types of PII that cannot be easily changed (such as dates of birth and Social Security numbers) are the most valuable to hackers.[6]

46. Defendant knew or should have known that it was an ideal target for hackers and others with nefarious purposes related to sensitive personal identifying and health information.

[6] *Calculating the Value of a Data Breach – What Are the Most Valuable Files to a Hacker?* Donnellon McCarthy Enters. (July 21, 2020), https://www.dme.us.com/2020/07/21/calculating-the-value-of-a-data-breach-what-are-the-most-valuable-files-to-a-hacker/.

Defendant processed and saved multiple types, and many levels, of PII and PHI through its computer data and storage systems.

47. Indeed, the Federal Bureau of Investigation ("FBI") has expressed concerned about data security in the healthcare industry. The FBI has been warning companies within the healthcare industry, like Defendant, that hackers are targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PHI)."[7]

48. The American Medical Association ("AMA") has also warned healthcare companies like Defendant about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[8]

49. Healthcare related breaches have continued to rapidly increase because electronic patient data is seen as a valuable asset. According to the 2019 HIMSS Cybersecurity Survey, 82% of participating hospital information security leaders reported having a significant security incident in the last 12 months, with a majority of these known incidents being caused by "bad actors" such

---

[7] Jim Finkle, *FBI warns healthcare firms that they are targeted by hackers*, REUTERS (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820.

[8] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AMA (Oct. 4, 2016), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals.

as cybercriminals.[9] "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[10]

50. As major healthcare service administrator, Defendant knew, or should have known, the importance of safeguarding the patients' PII and PHI entrusted to it and of the foreseeable consequences if that data was disclosed. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

51. By requiring the production of, collecting, obtaining, using, and deriving benefits from Plaintiff' and Class Members' PII and PHI, Defendant assumed certain legal and equitable duties, and it knew or should have known that it was responsible for the diligent protection of that PII and PHI it collected and stored.

52. Defendant had the resources and responsibility to invest in the necessary data security and protection measures. Yet, Defendant failed to undertake adequate analyses and testing of its own systems and other data security measures to avoid the failures that resulted in the Data Breach.

53. The seriousness with which Defendant should have taken its data security is shown by the number of data breaches perpetrated in the healthcare, banking, and retail industries over the past few years.

---

[9] *2019 HIMSS Cybersecurity Survey*, https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf (last visited June 2, 2023).

[10] Eyal Benishti, *How to Safeguard Hospital Data from Email Spoofing Attacks*, Chief Healthcare Executive (Apr. 4, 2019), https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks.

54. Over 41 million patient records were breached in 2019, with a single hacking incident affecting close to 21 million records.[11] Healthcare breaches in 2019 almost tripled those the healthcare industry experienced in 2018, when 15 million patient records were affected by data breach incidents.[12]

55. Protenus, a healthcare compliance analytics firm, analyzed data breach incidents disclosed to the U.S. Department of Health and Human Services or the media during 2019, finding that there has been an alarming increase in the number of data breaches of patient privacy since 2016, when there were 450 security incidents involving patient data.[13] In 2019 that number jumped to 572 incidents, which is likely an underestimate. There continues to be on average at least one health data breach every day.[14]

56. One recent report found that in 2020, healthcare was one of the industries most affected by tracked ransomware incidents.[15]

Defendant's Conduct Violates HIPAA and Industry Standard Data Security Practices.

57. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for

---

[11] Heather Landi, *Number of patient records breached nearly triples in 2019*, FIERCE HEALTHCARE (Feb. 20, 2020), https://www.fiercehealthcare.com/tech/number-patient-records-breached-2019-almost-tripled-from-2018-as-healthcare-faces-new-threats.

[12] *Id*.

[13] *Id*.

[14] *Id.*

[15] Kat Jerich, *Healthcare hackers demanded an average ransom of $4.6M last year, says BakerHostetler*, HEALTHCARE IT NEWS (May 4, 2021), https://www.healthcareitnews.com/news/healthcare-hackers-demanded-average-ransom-46m-last-year-says-bakerhostetler.

handling PHI like the data left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

58. The Data Breach resulted from a combination of insufficiencies that indicate Defendant failed to comply with safeguards mandated by HIPAA regulations and industry standards. The security failures include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to adequately catalog the location of Plaintiff's and Class Members' digital information;

d. Failing to properly encrypt Plaintiff's and Class Members' PHI;

e. Failing to ensure the confidentiality and integrity of electronic PHI Defendant create, receive, maintain, and transmit in violation of 45 C.F.R. §164.306(a)(1);

f. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. §164.312(a)(1);

g. 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);

h. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. §164.308(a)(6)(ii);

i. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. §164.306(a)(2);

j. Failing to protect against any reasonably-anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. §164.306(a)(3);

k. Failing to ensure compliance with HIPAA security standard rules by their workforce in violation of 45 C.F.R. §164.306(a)(94);

l. Impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons in violation of 45 C.F.R. §164.502, *et seq.*;

m. Failing to effectively train all members of their workforce (including

independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. §164.530(b) and 45 C.F.R. §164.308(a)(5); and

n. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. §164.530(c).

Defendant Acknowledge the Harm this Data Breach Has and Will Cause the Victims.

59. It is highly probable that the criminal(s) that breached Defendant' systems and acquired Plaintiff' and Class Members' PII and PHI did so for the purpose of using that data to commit fraud, theft, and other crimes, or for the purpose of selling or providing the PII and PHI to other individuals intending to commit fraud, theft, and other crimes. This is made clear by the fact that the stolen data was posted to the dark web.

60. Plaintiff and Class Members have already suffered injury and face a substantial risk for imminent and certainly impending future injury.

61. Defendant acknowledges the risk of fraud, theft, and other crimes faced by victims of the Data Breach in its notices to Plaintiff and Class Members.

62. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[16] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[17]

[16] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013), https://www.justice.gov/usao-wdmi/file/764151/download.

[17] *See id*. 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(a). 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

63. The physical, emotional, and social toll suffered (in addition to the financial toll) by identity theft victims cannot be understated.[18] "A 2016 Identity Theft Resource Center survey of identity theft victims sheds light on the prevalence of this emotional suffering caused by identity theft: 74 percent of respondents reported feeling stressed[,] 69 percent reported feelings of fear related to personal financial safety[,] 60 percent reported anxiety[,] 42 percent reported fearing for the financial security of family members[, and] 8 percent reported feeling suicidal."[19]

64. More recently, the FTC released an updated publication on protecting PII for businesses, which includes instructions on protecting PII, properly disposing of PII, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

65. The FTC has, upon information and belief, brought enforcement actions against businesses for failing to protect consumers' PII and PHI. The FTC has done this by treating a failure to employ reasonable measures to protect against unauthorized access to PII and PHI as a violation of the FTC Act, 15 U.S.C. §45.

66. Identity thieves may commit various types of crimes such as, *inter alia*, immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, fraudulently obtaining medical services, and/or using the victim's information to obtain a fraudulent tax refund.

---

identification number, alien registration number, government passport number, employer or taxpayer identification number." 16 C.F.R. §603.2(b)

[18] Alison Grace Johansen, *4 Lasting Effects of Identity Theft*, NortonLifeLock (Mar. 13, 2018), https://www.lifelock.com/learn-identity-theft-resources-lasting-effects-of-identity-theft.html.

[19] *Id.* (citing *Identity Theft: The Aftermath 2016™*, Identity Theft Resource Center (2016) https://www.idtheftcenter.org/images/page-docs/AftermathFinal_2016.pdf).

67. The United States government and privacy experts acknowledge that it may take much time for identity theft to come to light and be detected because identity thieves may wait years before using the stolen data.

68. Because the information Defendant allowed to be compromised and taken is of such a durable and permanent quality (*i.e.*, names, Social Security numbers, dates of birth, and PHI), the harms to Plaintiff and the Class will continue and increase, and Plaintiff and the Class will continue to be at substantial risk for further imminent and future harm.

Plaintiff's and Class Members' PII and PHI Are Very Valuable.

69. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[20] 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."[21] The FTC acknowledges that identity theft victims must spend countless hours and large amounts of money repairing the impact to their good name and credit record.[22]

70. Consumers rightfully place a high value not only on their PII and PHI, but also on the privacy of that data. Researchers have already begun to shed light on how much consumers value their data privacy – and the amount is considerable. Notably, one study on website privacy determined that U.S. consumers valued the restriction of improper access to their personal information – the very injury at issue here – between $11.33 and $16.58 per website. The study

---

[20] 17 C.F.R §248.201.

[21] *Id.*

[22] *Guide for Assisting Identity Theft Victims*, FTC (Sep. 2013), https://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf (the "FTC Guide").

also determined that "[a]mong U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US$30.49 – 44.62."[23] This study was done in 2002, almost twenty years ago. The sea-change in how pervasive the Internet is in everyday lives since then indicates that these values—when associated with the loss of PII and PHI to bad actors—would be exponentially higher today.

71. The unauthorized disclosure of Social Security numbers can be particularly damaging, because Social Security numbers cannot easily be replaced. In order to obtain a new Social Security number a person must prove, among other things, that he or she continues to be disadvantaged by the misuse. Thus, no new Social Security number can be obtained until the damage has been done.

72. Furthermore, as the Social Security Administration ("SSA") warns:

> Keep in mind that a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal 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 personal 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 information isn't 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.[24]

---

[23] Il-Horn Hann, Kai-Lung Hui, *et al.*, *The Value of Online Information Privacy: Evidence from the USA and Singapore*, at 17. Marshall Sch. Bus., Univ. So. Cal. (Oct. 2002), https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf.

[24] SSA, *Identity Theft and Your Social Security Number*, SSA Publ'n No. 05-10064 (Dec. 2013), http://www.ssa.gov/pubs/EN-05-10064.pdf.

73. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns.[25] Victims of the Data Breach, including Plaintiff, will spend, and already have spent, time contacting various agencies, such as the Internal Revenue Service and the SSA. They also now face a real and imminent substantial risk of identity theft and other problems associated with the disclosure of their Social Security number and will need to monitor their credit and tax filings for an indefinite duration.

74. PHI is just as, if not more, valuable than Social Security numbers. According to a report by the FBI's Cyber Division, healthcare records can be sold by criminals for 50 times the price of stolen Social Security numbers or credit card numbers.[26] A file containing private health insurance information can be bought for between $1,200 and $1,300 ***each*** on the black market.[27]

75. PII and PHI are valuable commodities to thieves. PHI is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market," commonly referred to as the dark web, for a number of years.[28] As a result of large-scale data breaches, identity thieves and cyber criminals have openly posted stolen Social Security numbers, healthcare information, and other PHI directly on various Internet websites making the information publicly available. These networks and

---

[25] When fraudulent tax returns are filed, the requirements for a legitimate taxpayer to file their tax returns with the IRS increase, including the necessity to obtain and utilize unique PIN numbers just to be able to file a tax return.

[26] *FBI Cyber Division Bulletin: Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusion*, FBI (Apr. 8, 2014), https://publicintelligence.net/fbi-health-care-cyber-intrusions/.

[27] Elizabeth Clarke, *Hackers Sell Health Insurance Credentials, Bank Accounts, SSNs and Counterfeit Documents*, SECUREWORKS (July 15, 2013), https://www.secureworks.com/blog/general-hackers-sell-health-insurance-credentials-bank-accounts-ssns-and-counterfeit-documents

[28] FTC Guide, *supra* n.31.

markets consist of hundreds of thousands, if not millions, of nefarious actors who view and access the PHI.

76. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identity theft, and medical and financial fraud.[29]

77. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

78. Legitimate companies also recognize that PII and PHI are valuable assets. Some companies recognize PII, and especially PHI, as a close equivalent to personal property. Software has been created by companies to value a person's identity on the black market. The commoditization of this information is thus felt by consumers as theft of personal property in addition to an invasion of privacy.

79. Thus, the compromised PII and PHI of Plaintiff and Class Members have a high value on both legitimate and black markets.

80. Moreover, compromised health information can lead to falsified information in medical records and fraud that can persist for years as it "is also more difficult to detect, taking twice as long as normal identity theft."[30]

81. Because the information Defendant allowed to be compromised and taken is of such a durable and permanent quality, the harms to Plaintiff and Class Members will continue and

---

[29] *Warning Signs of Identity Theft*, FTC https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft (last visited Apr. 19, 2021).

[30] *See* FBI, *supra* n.35.

increase, and Plaintiff and Class Members will continue to be at substantial risk for further imminent and future harm.

Defendant's Post-Breach Activity Was (and Remains) Inadequate.

82. Immediate notice of a security breach is essential to protect victims such as Plaintiff and Class Members. Plaintiff did not receive notice of the Data Breach until three months after the Data Breach was discovered (an unreasonable amount of time by any measure), thus further exacerbating the harm Plaintiff and Class Members suffered as a result of the Data Breach.

83. Such failure to protect Plaintiff's and Class Members' PII and PHI, and the delay in their notification of the Data Breach, has significant ramifications. The information stolen allows criminals to commit theft, identity theft, and other types of fraud. Moreover, because the data points stolen are persistent—for example, names, dates of birth, Social Security numbers, and health insurances data—as opposed to transitory, criminals who access, steal, or purchase the PII and PHI belonging to Plaintiff and Class Members, do not need to use the information to commit fraud immediately. The PII and PHI can be used or sold for use years later, and often is.

84. Plaintiff and Class Members are now at a significant risk of imminent and future fraud, misuse of their PII and PHI, and identity theft for many years in the future as a result of the Defendant' actions and the Data Breach. The theft of their PHI is particularly impactful, as many banks or credit card providers have substantial fraud detection systems with quick freeze or cancellation programs in place, whereas the breadth and usability of PHI allows criminals to get away with misuse for years before healthcare-related fraud is spotted.

85. Plaintiff and Class Members have suffered real and tangible losses, including but not limited to the loss in the inherent value of their PII and PHI, the loss of their time as they have had to spend additional time monitoring accounts and activity, and additional economic loss to mitigate the costs of injuries realized as a result of discovery in this case, but until recently, kept

silent by Defendant.

86. Despite Defendant' failure to protect Plaintiff's and Class Members' PII and PHI, they have only offered to provide them with trivial compensation or an inadequate remedy, such as free credit monitoring or identity protection services. Upon information and belief, Plaintiff and Class Members also were not offered or provided any adequate compensation or remedy to protect their information taken in this Data Breach.

Plaintiff and Class Members Suffered Long-Lasting Damages.

87. The ramifications of Defendant's failure to keep Plaintiff's and Class Members' PII and PHI secure are long lasting and severe. Once PII and PHI are stolen, fraudulent use of that information and damage to victims may continue for years.

88. Criminals often trade stolen PII and PHI on the "cyber black-market" for years following a breach. Cybercriminals can post stolen PHI on the internet, thereby making such information publicly available. These cybercriminals and other unauthorized third parties are now free to exploit and misuse that PII and PHI without any ability for Plaintiff and Class Members to recapture and erase the PII and PHI from further dissemination. Plaintiff's and Class Members' PII and PHI is forever compromised, and this PII and PHI were unique to the information that Defendant inadequately and improperly safeguarded.

89. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened.[31] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that

[31] *See* Donna Parent, *Medical ID Theft Checklist*, IDENTITYFORCE (May 18, 2019), https://www.identityforce.com/blog/medical-id-theft-checklist-2.

were incurred in their names.[32]

90. Healthcare related data is among the most sensitive and personally consequential when compromised. A report focusing on health-care breaches found that the "average total cost to resolve an identity theft-related incident…came to about $20,000."[33] Further, a majority of the victims were forced to pay out-of-pocket costs for health care they did not receive in order to restore coverage. Moreover, almost 50% of the victims lost their health care coverage as a result of the incident, while nearly one-third said their insurance premiums went up after the event. Forty percent of the victims were never able to resolve their identity theft at all. Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.[34]

91. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to

---

[32] *The Potential Damages and Consequences of Medical Identity Theft and Healthcare Data Breaches*, EXPERIAN (Apr. 2010), https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

[33] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010) https://www.cnet.com/tech/services-and-software/study-medical-identity-theft-is-costly-for-victims/.

[34] *Id.*

their personal medical files due to the thief's activities."[35]

92. Here, not only was sensitive medical information divulged and compromised, but also patient Social Security numbers were involved. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later.[36] This time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used, compounds an identity theft victim's ability to detect and address the harm.

93. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

94. Moreover, according to Robert P. Chappell, Jr., a law enforcement professional, a minor's information can be stolen and used until the minor turns eighteen years old before the minor even realizes he or she has been victimized.[37]

95. The risk to Class Members who are children is substantial given their age and lack

---

[35] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," KAISER HEALTH NEWS, (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft/.

[36] *Identity Theft and Your Social Security Number*, SSA (June 2018), http://www.ssa.gov/pubs/EN-05-10064.pdf.

[37] Brett Singer, *What is Child Identify Theft?*, Parents, https://www.parents.com/kids/safety/tips/what-is-child-identity-theft/ (last visited July 28, 2021).

of established credit because their information can be used to create a "clean identity slate." It is not surprising then that one report found that children are 51% more likely be victims of identity theft than adults.[38] Cybercriminals on the Dark Web have been caught selling Social Security numbers of infants for $300 per number to be used on fraudulent tax returns.[39]

96. The PII and PHI belonging to Plaintiff and Class Members is private and sensitive in nature and was left inadequately protected by Defendant who did not obtain Plaintiff' or Class Members' consent to disclose their PII and PHI to any other person as required by applicable law and industry standards. The Data Breach was a direct and proximate result of Defendant' failure to: (a) properly safeguard and protect Plaintiff's and Class Members' PII and PHI from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' PII and PHI; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

97. Had Defendant remedied the deficiencies in its data security system and adopted security measures and protocols recommended by experts in the field, Defendant would have prevented the intrusion and, ultimately, the theft of PII and PHI.

98. As a direct and proximate result of Defendant's wrongful actions and inaction, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which

---

[38] Avery Wolfe, *How Data Breaches Affect Children*, Axion Cyber Sols. (Mar. 15, 2018), https://axiomcyber.com/data-breach/how-data-breaches-affect-children/.

[39] *Id.*

they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

99. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "[r]esolving the problems caused by identity theft [could] take more than a year for some victims."[40]

100. As a result of the Defendant' failure to prevent the Data Breach, Plaintiff and Class Members have suffered, will suffer, or are at increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their PII and PHI;

b. Unauthorized use and misuse of their PII and PHI;

c. The loss of the opportunity to control how their PII and PHI are used;

d. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages and time associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

f. The imminent and certain impending injury flowing from potential fraud and identity theft posed by their PII and PHI being placed in the hands of criminals;

g. The continued risk to their PII and PHI that is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the PII and PHI in its possession; and

[40] Erika Harrell, Ph.D. and Lynn Langton, Ph.D., *Victims of Identity Theft, 2012*, DOJ, Off. of Just. Programs, Bureau of Just. Statistics (Dec. 2013), https://www.bjs.gov/content/pub/pdf/vit12.pdf.

h. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

101. In addition to a remedy for the economic harm, Plaintiff and the Class maintain an undeniable and continuing interest in ensuring that their PII and PHI that remains in the possession of Defendant is secure, remains secure, and is not subject to further theft

CLASS ACTION ALLEGATIONS

102. Pursuant to the provisions of Fed. R. Civ. P. 23(a), 23(b)(1), 23(b)(2), 23(b)(3), and 23(c)(4), Plaintiff seeks to bring this class action on behalf of himself and a nationwide class (the "Nationwide Class") defined as follows:

All persons who reside in the United States whose PII and PHI were accessed and divulged by the Data Breach.

103. The Nationwide Class asserts claims against Defendant for negligence, unjust enrichment, and breach of implied contract.

104. Excluded from the Class are Defendant; officers, directors, and employees of Defendant; any entity in which Defendant have a controlling interest, is a parent or subsidiary, or which is controlled by Defendant; and the affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assigns of Defendant. Also excluded are the Judges and Court personnel in this case and any members of their immediate families.

105. Plaintiff reserves the right to modify and/or amend the Nationwide Class definition, including but not limited to creating additional subclasses, as necessary.

106. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of the 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.

107. All Class Members are readily ascertainable in that Defendant have access to

addresses and other contact information for all Class Members, which can be used for providing notice to Class Members.

108. ***Numerosity***. Consistent with Fed. R. Civ. P. 23(a)(1), the Nationwide Class is so numerous that joinder of all members is impracticable. While the exact number of Nationwide Class Members is unknown, upon information and belief, it is in excess of 8.9 million.

109. ***Commonality and Predominance***. Consistent with Fed. R. Civ. P. 23(a)(2) and (b)(3), this action involves common questions of law and fact that predominate over any questions that may affect only individual Class Members. Such common questions include:

a. whether Defendant engaged in the wrongful conduct alleged in this Complaint;

b. whether Defendant's conduct was unfair, unconscionable, and/or unlawful;

c. whether Defendant failed to implement and maintain adequate and reasonable systems and security procedures and practices to protect Plaintiff' and Class Members' PII and PHI;

d. whether Defendant owed a duty to Plaintiff and Class Members to adequately protect their PII and PHI and to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

e. whether Defendant breached their duties to protect the PII and PHI of Plaintiff and Class Members by failing to provide adequate data security and failing to provide appropriate and adequate notice of the Data Breach to Plaintiff and Class Members;

f. whether Defendant's conduct was negligent;

g. whether Defendant knew or should have known that its computer systems were vulnerable to being compromised;

h. whether Defendant' conduct, including their failure to act, resulted in or was the proximate cause of the Data Breach of their systems, resulting in the loss of Plaintiff' and Class Members' PII and PHI;

i. whether Defendant wrongfully or unlawfully failed to inform Plaintiff and Class Members that it did not maintain computers and security practices adequate to reasonably safeguard Plaintiff's and Class Members' PII and PHI;

j. whether Plaintiff and Class Members suffered injury, including ascertainable losses, as a result of Defendant's conduct (or failure to act);

k. whether Plaintiff and Class Members are entitled to recover damages; and

l. whether Plaintiff and Class Members are entitled to declaratory relief and equitable relief, including injunctive relief, restitution, disgorgement, and/or other equitable relief.

110. ***Typicality***. Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiff's claims are typical of the claims of other Class Members in that Plaintiff, like all Class Members, had their PII and PHI compromised, breached, and stolen in the Data Breach. Plaintiff and all Class Members were injured through the misconduct of Defendant, described in this Complaint, and assert the same claims for relief.

111. ***Adequacy***. Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiff and counsel will fairly and adequately protect the interests of the Class. Plaintiff is a member of the Class he seeks to represent, is committed to pursuing this matter against Defendant to obtain relief for the Class; and has no interests that are antagonistic to, or in conflict with, the interests of other Class Members. Plaintiff retained counsel who are competent and experienced in litigating class actions and complex litigation, including privacy litigation of this kind. Plaintiff and his counsel intend to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

112. ***Superiority***. Consistent with Fed. R. Civ. P. 23(b)(3), a class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most Class Members would find the cost of litigating their claims prohibitively high and would therefore have no effective remedy, so that in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the Class. Plaintiff and Class Members have been

harmed by Defendant's wrongful conduct and/or action. Litigating this action as a class action will reduce the possibility of repetitious litigation relating to Defendant's conduct and/or inaction. Plaintiff knows of no difficulties that would be encountered in this litigation that would preclude its maintenance as a class action.

113. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(b)(3), because the common questions of law or fact predominate over any questions affecting individual Class Members, a class action is superior to other available methods for the fair and efficient adjudication of this controversy, and the requirements of Rule 23(a) are met.

114. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(1), in that the prosecution of separate actions by the individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action conserves judicial resources and the parties' resources and protects the rights of each Class Member. Specifically, injunctive relief could be entered in multiple cases, but the ordered relief may vary, causing Defendant to have to choose between differing means of upgrading its data security infrastructure and choosing the court order with which to comply. Class action status is also warranted because prosecution of separate actions by Class Members would create the risk of adjudications with respect to individual Class Members that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

115. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2) because Defendant, through its uniform conduct, acted or failed and refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class

as a whole. Moreover, Defendant continues to maintain its inadequate security practices, retain possession of Plaintiff's and Class Members' PII and PHI, and has not been forced to change its practices or to relinquish PII and PHI by nature of other civil suits or government enforcement actions, thus making injunctive relief a live issue and appropriate to the Class as a whole.

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

a. whether Plaintiff's and Class Members' PII and PHI were accessed, compromised, or stolen in the Data Breach;

b. whether Defendant owed a legal duty to Plaintiff and the Class Members;

c. whether Defendant failed to take adequate and reasonable steps to safeguard the PII and PHI of Plaintiff and Class Members;

d. whether Defendant failed to adequately monitor their data security systems;

e. whether Defendant failed to comply with applicable laws, regulations, and industry standards relating to data security;

f. whether Defendant knew or should have known that it did not employ adequate and reasonable measures to keep Plaintiff's and Class members' PII and PHI secure; and

g. whether Defendant's adherence to HIPAA regulations, FTC data security obligations, industry standards, and measures recommended by data security experts would have reasonably prevented the Data Breach.

COUNT I

Negligence

On Behalf of Plaintiff and the Nationwide Class

117. Plaintiff realleges and incorporates by reference paragraphs 1-116 of the Complaint as if fully set forth herein.

118. Plaintiff brings this claim on behalf of himself and the Nationwide Class.

119. Defendant collected, stored, used, and benefited from the non-public PII and PHI of Plaintiff and Class Members in the procurement and provision of dental service benefits for Plaintiff and Class Members.

120. Defendant had full knowledge of the sensitivity of the PII and PHI and the types of harm that Plaintiff and Class Members could and would suffer if the PII and PHI were wrongfully disclosed.

121. By collecting, storing, and using Plaintiff's and Class Members' PII and PHI, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, securing, deleting, protecting, and safeguarding the sensitive PII and PHI. Defendant owed a duty to prevent the PII and PHI it received from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

122. Defendant was required to prevent foreseeable harm to Plaintiff and Class Members, and it therefore had a duty to take adequate and reasonable steps to safeguard sensitive PII and PHI from unauthorized release or theft. This duty included: (1) designing, maintaining, and testing its data security systems, data storage architecture, and data security protocols to ensure Plaintiff's and Class Members' PII and PHI in its possession was adequately secured and protected; (2) implementing processes that would detect an unauthorized breach of its security systems and data storage architecture in a timely and adequate manner; (3) timely acting on all warnings and alerts, including public information, regarding its security vulnerabilities and potential compromise of the PII and PHI of Plaintiff and Class Members; and (4) maintaining data security measurers consistent with industry standards and applicable federal and state laws and other requirements.

123. Defendant had a common law duty to prevent foreseeable harm to Plaintiff and

Class Members. The duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices of Defendant in its collection, storage, and use of PII and PHI from Plaintiff and Class Members. In fact, not only was it foreseeable that Plaintiff and Class Members would be harmed by the failure to protect their PII and PHI because malicious actors routinely attempt to steal such information for use in nefarious purposes, but Defendant also knew that it was more likely than not Plaintiff and Class Members would be harmed as a result.

124. Defendant's duties to use adequate and reasonable security measures also arose as a result of the special relationship that existed between it, on the one hand, and Plaintiff and Class Members, on the other hand. This special relationship arose because Defendant collected, stored, and used the PII and PHI of Plaintiff and Class Members for the procurement and provision of health services for Plaintiff and Class Members. Defendant alone could have ensured that its security systems and data storage architecture were sufficient to prevent or minimize the Data Breach.

125. Additionally, the policy of preventing future harm weighs in favor of finding a special relationship between Defendant and Plaintiff and Class Members. If companies are not held accountable for failing to take adequate and reasonable security measures to protect the sensitive PII and PHI in their possession, they will not take the steps that are necessary to protect against future security breaches.

126. Defendant also owed a duty to timely disclose the material fact that its computer systems and data security practices and protocols were inadequate to safeguard users' personal, health, and financial data from theft.

127. The injuries suffered by Plaintiff and Class Members were proximately and directly

caused by Defendant's failure to follow reasonable, industry standard security measures to protect Plaintiff's and Class Members' PII and PHI.

128. When individuals have their personal information stolen, they are at substantial risk for imminent identity theft, and need to take steps to protect themselves, including, for example, buying credit monitoring services and purchasing or obtaining credit reports to protect themselves from identity theft.

129. If Defendant had implemented the requisite, industry standard security measures and exercised adequate and reasonable care, data thieves would not have been able to take the PII and PHI of Plaintiff and Class Members.

130. Defendant breached these duties through the conduct alleged here by, including without limitation, failing to protect the PII and PHI in their possession; failing to maintain adequate computer systems and allowing unauthorized access to and exfiltration of Plaintiff's and Class Members' PII and PHI; failing to disclose the material fact that Defendant's computer systems and data security practices were inadequate to safeguard the PII and PHI in its possession from theft; and failing to disclose in a timely and accurate manner to Plaintiff and Class Members the material fact of the Data Breach.

131. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII and PHI would not have been compromised. And as a direct and proximate result of Defendant's failure to exercise adequate and reasonable care and use commercially adequate and reasonable security measures, the PII and PHI of Plaintiff and Class Members were accessed by ill-intentioned individuals who could and will use the information to commit identity or financial fraud. Plaintiff and Class Members face the imminent, certainly impending, and substantially heightened risk of identity theft, fraud, and further misuse of their

personal data.

132. There is a temporal and close causal connection between Defendant's failure to implement security measures to protect the PII and PHI of current and former patients and the harm suffered, or risk of imminent harm suffered, by Plaintiff and Class Members.

133. It was foreseeable that Defendant's failure to exercise reasonable care to safeguard the PII and PHI in its possession or control would lead to one or more types of injury to Plaintiff and Class Members. And the Data Breach was foreseeable given the known, high frequency of cyberattacks and data breaches in the healthcare industry.

134. Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew of or should have known of the inherent risks in collecting and storing PII and PHI, the critical importance of providing adequate security of PII and PHI, the current cyber scams being perpetrated on PII and PHI, and that it had inadequate protocols, including security protocols in place to secure the PII and PHI of Plaintiff and Class Members.

135. Plaintiff and Class Members have no ability to protect their PII and PHI that was and is in Defendant's possession. Defendant alone was and is in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

136. As a direct and proximate result of Defendant's negligence as alleged above, Plaintiff and Class Members have suffered, will suffer, or are at increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their PII and PHI;

b. Unauthorized use and misuse of their PII and PHI;

c. The loss of the opportunity to control how their PII and PHI are used;

d. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages and time associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

f. The imminent and certain impending injury flowing from potential fraud and identity theft posed by their PII and PHI being placed in the hands of criminals;

g. The continued risk to their PII and PHI that is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the PII and PHI in its possession; and

h. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

137. Pursuant to the FTC Act, 15 U.S.C. §45, Defendant had a duty to provide fair and adequate computer systems and data security measures to safeguard the PII and PHI of Plaintiff and Class Members.

138. The FTC Act prohibits "unfair . . . practices in or affecting commerce," which the FTC has interpreted to include businesses' failure to use reasonable measures to protect PII and PHI. The FTC publications and orders described above also form part of the basis of Defendant' duty in this regard. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

139. Defendant solicited, gathered, and stored PII and PHI of Plaintiff and Class Members to facilitate transactions which affect commerce.

140. Defendant violated the FTC Act (and similar state statutes) and HIPAA, by failing to use reasonable measures to protect PII and PHI of Plaintiff and Class Members and not complying with applicable industry standards, as described herein. Defendant's conduct was

particularly unreasonable given the nature and amount of PII and PHI obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

141. Defendant' violations of the FTC Act (and similar state statutes) and HIPAA are evidence of negligence.

142. Plaintiff and Class Members are within the class of persons that the FTC Act and HIPAA were intended to protect.

143. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act and HIPAA were intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ adequate and reasonable data security measures caused the same harm as that suffered by Plaintiff and Class Members.

144. As a direct and proximate result of Defendant' violations of the above-mentioned statutes (and similar state statutes), Plaintiff and Class Members have suffered, and continue to suffer, damages arising from the Data Breach as described herein and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT II

Breach of Implied Contract

On Behalf of Plaintiff and the Nationwide Class

145. Plaintiff realleges and incorporates by reference paragraphs 1 through 116 as if fully set forth herein.

146. In connection with receiving health care services, Plaintiff and Class members entered into implied contracts with Defendant.

147. Pursuant to these implied contracts, Plaintiff and Class members performed a benefit for Defendant by directly or indirectly paying monies to Defendant and providing Defendant with their sensitive PII and PHI. In exchange for this benefit, Defendant agreed to,

among other things, provide health care services to Plaintiff and Class Members, take reasonable measures to protect the security and confidentiality of Plaintiff's and Class Members' PII and PHI, protect Plaintiff's and Class members' PII and PHI in compliance with federal and state laws and regulations and industry standards, and implement and maintain reasonable measures to protect the security and confidentiality of Plaintiff's and Class Members' PII and PHI.

148. Protecting Plaintiff and Class Members' PII and PHI was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and Defendant on the other hand. Indeed, Defendant recognized the importance of data security and the privacy of their patients' PII and PHI.

149. Had Plaintiff and Class members known that Defendant would not adequately protect their PII and PHI, they would not have paid Defendant for its services.

150. Plaintiff and Class Members performed their obligations under the implied contracts when they provided Defendant with their PII and PHI and paid monies for products and services from Defendant, expecting that their PII/PHI would be protected.

151. Defendant breached its obligations under its implied contracts with Plaintiff and Class members by failing to implement and maintain reasonable security measures to protect and secure their PII/PHI, and in failing to implement and maintain adequate security protocols and procedures to protect Plaintiff's and Class members' PII/PHI in a manner that complies with applicable laws, regulations, and industry standards.

152. Defendant's breach of its obligations of the implied contracts with Plaintiff and Class Members directly resulted in the Data Breach and the resulting injuries to Plaintiff and Class members.

153. Plaintiff and all other Class members were damaged by Defendant's breach of

implied contracts because they paid monies (directly or indirectly) to Defendant in exchange for data security protection they did not receive; they now face a substantially increased and imminent risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; their PII and PHI was improperly disclosed to unauthorized individuals; the confidentiality of their PII and PHI has been breached; they were deprived of the value of their PII and PHI, for which there is a well-established national and international market; they lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and, they overpaid for the services that they received.

COUNT III

Unjust Enrichment

On Behalf of Plaintiff and the Nationwide Class

154. Plaintiff realleges and incorporates by reference paragraphs 1 through 116 as if fully set forth herein.

155. In obtaining services from Defendant, Plaintiff and Class Members provided and entrusted their PII and PHI to Defendant.

156. Plaintiff and Class members conferred a monetary benefit upon Defendant in the form of monies paid for Dental Services with an implicit understanding that Defendant would use some of that income to protect the PII and PHI it collects, retains, and stores.

157. Defendant accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. Defendant benefitted from the collection of Plaintiff's and Class members' PII and PHI, as this was used to facilitate billing and payment services, which enabled MCNA to conduct business.

158. As a result of Defendant's conduct, Plaintiff and Class members suffered actual

damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class Members paid for and expected, and those payments without reasonable data privacy and security practices and procedures that they received.

159. It is unjust for MCNA to retain the money belonging to Plaintiff and Class Members because Defendant failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class Members paid for and reasonably expected, and that were otherwise mandated by both law and industry standards.

160. Defendant should be ordered to provide for the benefit of Plaintiff and Class Members all unlawful proceeds it received as a result of the conduct and Data Breach alleged in this Complaint.

RELIEF REQUESTED

WHEREFORE, Plaintiff, individually and on behalf of the proposed Class, respectfully requests the following relief:

a. An order certifying this case as a class action on behalf of the Class, defined above, appointing Plaintiff as Class representatives and appointing the undersigned counsel as Class counsel;

b. A mandatory permanent injunction directing Defendant to adequately safeguard Plaintiff's and the Class' PII and PHI by implementing improved security procedures and measures as outlined above;

c. An award of other declaratory, injunctive, and equitable relief as is necessary to protect the interests of Plaintiff and Class Members;

d. An award of restitution and compensatory, consequential, and general damages to Plaintiff and Class Members, including nominal damages as allowed by law in an

amount to be determined at trial or by this Court;

e. An award of actual or statutory damages to Plaintiff and Class Members in an amount to be determined at trial or by this Court;

f. An award of reasonable litigation expenses and costs and attorneys' fees to the extent allowed by law;

g. An award to Plaintiff and Class Members of pre- and post-judgment interest, to the extent allowable; and

h. Award such other and further relief as equity and justice may require.

JURY TRIAL DEMANDED

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of any and all issues in this action so triable as of right.

Dated: June 14, 2023

Respectfully submitted,

s/ John A. Yanchunis

MORGAN & MORGAN
COMPLEX LITIGATION GROUP
JOHN A. YANCHUNIS
JEAN S. MARTIN *(pro hac vice)*
FRANCESCA KESTER
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Telephone: 813/223-5505
jyanchunis@forthepeople.com
fkester@forthepeople.com
jeanmartin@forthepeople.com