UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF FLORIDA

AMBER LANDRY individually and on behalf of all others similarly situated, Plaintiff, v. MANAGED CARE OF NORTH AMERICA, INC., d/b/a MCNA Dental, Defendant.	Case No. _____ **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Amber Landry, individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to herself and on information and belief as to all other matters, by and through undersigned counsel, bring suit against Defendant Managed Care of North America, Inc., d/b/a MCNA Dental ("MCNA" or "Defendant").

NATURE OF THE ACTION

1. This is a class action brought by Plaintiff on behalf of herself and all other individuals ("Class Members") who had their sensitive personal information ("PII") and protected health information ("PHI")—as defined by Health Insurance Portability and Accountability Act ("HIPPA")— disclosed to unauthorized third parties that accessed and removed the PII and PHI from MCNA's system between at least February 26, 2023 and March 7, 2023, if not longer (the "Data Breach"). The compromised PII and PHI includes the following: (1) first and last names; (2) dates of birth; (3) phone numbers; (4) email addresses; (5) social security numbers; (6) driver's license numbers and other government-issued ID numbers; (7) health insurance (plan information, insurance company, member number, Medicaid-Medicare ID numbers); care for teeth or braces (visits, dentist name, doctor name, past care, x-rays/photos, medicines, and treatment); and bills and insurance claims.

2. In May 2023, MCNA notified 8,923,662 individuals that it suffered the Data Breach and informed them that their PII and PHI was compromised thereby (the "Notice").[1]

3. According to the Notice—posted on the Maine Attorney General website[2]—on March 6, 2023, MCNA "became aware that an unauthorized party was able to access certain MCNA systems." The Notice states that MCNA responded to the incident by opening an investigation with the assistance of a third-party forensic firm, which revealed that an unauthorized actor obtained access to MCNA's systems between February 26, 2023, and March 7, 2023Thus, the Data Breach resulted from MCNA's failure to adequately protect and safeguard that offline set of patient data.

4. Despite learning of the Data Breach on March 6, 2023, MCNA waited nearly three months before notifying impacted individuals—at the end of May 2023—that their highly sensitive PII and PHI had been acquired by an unauthorized actor by way of the Data Breach.

5. MCNA owed a duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure. MCNA breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect its patients' PII/PHI from unauthorized access and disclosure.

6. As a result of MCNA's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII and PHI was accessed and

[1] An example of MCNA's Notice was uploaded to the Maine Attorney General's website, accessible at: https://apps.web.maine.gov/online/aeviewer/ME/40/895b95c8-abc8-41f1-8c3f-b0415575de56.shtml (last visited June 16, 2023).
[2] https://apps.web.maine.gov/online/aeviewer/ME/40/895b95c8-abc8-41f1-8c3f-b0415575de56/871548ce-318e-48dd-a3b9-6eec9ef88da9/document.html (last visited June 16, 2023).

disclosed by a malicious, unauthorized actor. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of herself and all similarly situated individuals whose PII and/or PHI was exposed as a result of the Data Breach, which MCNA learned of on or about March 6, 2023, but did not publicly disclose until the end of May 2023.

7. Plaintiff, on behalf of herself and all other Class members, asserts claims for negligence, negligence per se, unjust enrichment, breach of fiduciary duty, breach of confidence, invasion of privacy, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

8. Plaintiff Amber Landry is a citizen of the state of Louisiana and resides in La Place, Louisiana. Believing that all of her current and former healthcare providers would implement and maintain reasonable security and practices to protect her PII and PHI, Plaintiff provided this information to her providers that upon information and belief utilized MCNA's services. On May 26, 2023, MCNA sent Plaintiff a letter confirming that her PII and PHI was impacted by the Data Breach. In the letter, MCNA identified that the nature of the information involved includes her first and last name, date of birth, phone number, email addresses, social security number, driver's license number and other government-issued ID number, health insurance (plan information, insurance company, member number, Medicaid-Medicare ID numbers), care for teeth or braces (visits, dentist name, doctor name, past care, x-rays/photos, medicines, and treatment), and bills and insurance claims. Plaintiff has spent approximately two hours monitoring her accounts for fraudulent activity and will continue to expend further time doing so in the days, weeks, and months following the filing of this complaint.

9. Defendant Managed Care of North America, Inc., d/b/a MCNA Dental is a corporation formed under the laws of Florida and maintains its principal place of business at 3100

SW 145th Avenue, Suite 200, in Miramar, Florida 33027. MCNA describes itself as a "leading dental benefits manager committed to providing high quality services to state agencies and managed care organizations for their Medicaid, Children's Health Insurance Program (CHIP), and Medicare members" that serves "over 5 million children and adults."[3]

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(a) and (d), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of five million dollars ($5,000,000.00) and is a class action in which one or more Class Members are citizens of states different from Defendant.

11. The Court has personal jurisdiction over Defendant because it maintains its principal place of business in this judicial district, conducts significant business in Miramar, Florida, and/or otherwise has sufficient minimum contacts with and intentionally avails itself of the markets in Florida.

12. Venue properly lies in this district because, *inter alia*, Defendant maintains its principal place of business in this judicial district; transacts substantial business, has agents, and is otherwise located in this district; and/or a substantial part of the conduct giving rise to Plaintiff's claims occurred in this judicial district.

FACTUAL ALLEGATIONS

A. Overview of Defendant

[3] https://www.mcna.net/en/company-overview (last visited June 16, 2023).

13. MCNA states its mission "is to deliver value to our clients and providers by providing access, quality and service excellence that improves the oral health outcomes of our members"[4]

14. MCNA states its "services and programs are built to meet and exceed industry standards and best practices" for the "over 5 million children and adults" it serves.[5]

15. MCNA advertises on its website that it has "successfully completed an independent, third-party SOC 2 audit by the AICPA of the processes and controls that ensure the security and availability of our information management systems and data" and that "[t]hese certifications underscore our continuous commitment to operating under the highest quality standards in our industry and to ensuring the best service possible for our members, providers, and clients."[6]

16. In the regular course of its business, Defendant collects and maintains the PII and PHI of its customers' patients, former patients, patients' parents and guardians, and other individuals. That information includes: (1) patient demographic information (such as patient name, parent/guardian name, address, email address, and date of birth); (2) Social Security numbers ("SSNs"), (3) health insurance information; (4) medical and/or treatment information (dates of service, location, services requested or procedures performed, diagnosis, prescription information, and physician names); (5) billing and/or claims information (invoices, submitted claims and appeals, and patient account identifiers used by your provider); and (6) information of a parent or guardian.

B. The Data Breach

[4] https://www.mcna.net/en/company-overview/ (last visited June 16, 2023).
[5] *Id.*
[6] *Id.*

17. The Notice of the Data Breach disseminated by MCNA states that on May 26, 2023, MCNA became aware that an unauthorized party was able to access certain MCNA systems.[7]

18. The Notice states that MCNA "took immediate steps to contain the threat and engaged a third-party forensic firm to investigate the incident and assist with remediation efforts."[8] Through this investigation, MCNA "discovered that certain systems within the network may have been infected with malicious code" and that as a result of the malicious code, "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."[9]

19. MCNA's report of the Data Breach on the website of Maine's Attorney General states that during that time, the unauthorized actor acquired the PII and PHI of over 8.9 million individuals.[10]

20. Thus, the Data Breach resulted from MCNA's failure to adequately protect and safeguard the PII and PHI entrusted to it through its provision of various services to its healthcare provider clients.

21. Despite learning of the Data Breach on March 6, 2023, MCNA waited nearly three months before notifying impacted individuals—on March 26, 2023—that their highly sensitive PII and PHI had been acquired by an "unauthorized third party" by way of the Data Breach.

22. The Notice that Defendant sent to Plaintiff and the Class states that the information that was accessed included:

---

[7] https://apps.web.maine.gov/online/aeviewer/ME/40/895b95c8-abc8-41f1-8c3f-b0415575de56/871548ce-318e-48dd-a3b9-6eec9ef88da9/document.html (last visited June 16, 2023).
[8] *Id.*
[9] *Id.*
[10] https://apps.web.maine.gov/online/aeviewer/ME/40/895b95c8-abc8-41f1-8c3f-b0415575de56.shtml (last visited June 16, 2023).

(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.[11]

C. Defendant Knew that Criminals Target PII/PHI

23. At all relevant times, Defendant knew, or should have known, its customers' patients', Plaintiff's, and all other Class members' PII/PHI was a target for malicious actors. Despite such knowledge, Defendant failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' PII/PHI from cyber-attacks that Defendant should have anticipated and guarded against.

24. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2021 report, the healthcare compliance company Protenus found that there were 758 medical data breaches in 2020 with over 40 million patient records exposed.[12] This is an increase from the 572 medical data breaches that Protenus compiled in 2019.[13]

[11] https://apps.web.maine.gov/online/aeviewer/ME/40/895b95c8-abc8-41f1-8c3f-b0415575de56/871548ce-318e-48dd-a3b9-6eec9ef88da9/document.html (last visited June 16, 2023).
[12] Protenus, *2021 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/resources/2021-breach-barometer
[13] Protenus, *2020 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/resources/2020-breach-barometer

25. PII/PHI is a valuable property right.[14] The value of PII/PHI as a commodity is measurable.[15] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[16] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[17] It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

26. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, SSNs, PII/PHI, and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

27. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[18] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten

---

[14] *See* Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data

[15] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), http://www.medscape.com/viewarticle/824192.

[16] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD ILIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[17] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

[18] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAGAZINE (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon ("*What Happens to Stolen Healthcare Data* Article") (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for

personal identifying characteristics of an individual."[19] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[20]

28. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[21] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[22]

29. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[23] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[24]

---

criminals.").
[19] *Id.*
[20] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims.
[21] SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAGAZINE (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.
[22] Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.
[23] *What Happens to Stolen Healthcare Data*, *supra* at n.10.
[24] *Id.*

30. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[25]

31. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

D. Theft of PII/PHI Has Grave and Lasting Consequences for Victims

32. Theft of PII/PHI is serious. The FTC warns consumers that identity thieves use PII/PHI to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[26]

33. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[27] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things:

---

[25] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

[26] *See* Federal Trade Commission, *What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Nov. 15, 2021).

[27] 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*.

open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[28]

34. With access to an individual's PII/PHI, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[29]

35. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[30]

36. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to

[28] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (Sept. 1, 2017), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.
[29] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft.
[30] Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RESOURCE CENTER (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/.

demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

37. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[31]

38. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[32] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[33] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care."[34] The FTC also warns, "If the thief's health information is mixed with yours, your

[31] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.
[32] Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, FTC.GOV (Dec. 12, 2017), https://www.ftc.gov/system/files/documents/public_comments/2018/01/00037-142815.pdf
[33] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk*…, *supra* at n.14.
[34] *See* Federal Trade Commission, *What to Know About Medical Identity Theft*, Federal Trade Commission Consumer Information, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft.

treatment, insurance and payment records, and credit report may be affected."[35]

39. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.
- Significant bills for medical goods and services not sought nor received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.
- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information.
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[36]

40. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used and it takes some individuals up to three years to learn that information.[37]

---

[35] *Id*.
[36] *See* Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, *supra* at 24.
[37] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 Journal of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

41. It is within this harsh and dangerous reality that Plaintiff and all other Class members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

E. Damages Sustained by Plaintiff and the Other Class Members

42. Plaintiff and all other Class members have suffered injury and damages, including, but not limited to: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft and medical identity theft they face and will continue to face.

CLASS ALLEGATIONS

43. Plaintiff brings this action on behalf of herself and the following classes:

> Nationwide Class: All residents of the United States who were notified by Defendant that their PHI and PII may have been compromised as a result of the Data Breach.
>
> Louisiana Subclass: All residents of Louisiana who were notified by Defendant that their PHI and PII may have been compromised as a result of the Data Breach.

The foregoing classes are referred to herein, collectively, as the "Class."

44. Excluded from the Class are: (1) the Judges presiding over the Action, Class Counsel, and members of their families; (2) the Defendant, its subsidiaries, parent companies, successors, predecessors, and any entity in which Defendant or their parents, have a controlling interest, and their current or former officers and directors; (3) Persons who properly opt out; and (4) the successors or assigns of any such excluded Persons.

45. **Numerosity**: The Class is so numerous that joinder of all members is impracticable. According to Defendant, members of the Class are estimated to be over 8.9 million at this time.

46. **Typicality**: All of Plaintiff's claims are typical of the claims of the Class because the named Plaintiff, like all other members of the Classes, had her PII/PHI compromised in the Data Breach, such that all claims arise from the same uniform, core set of facts. Thus, Plaintiff is advancing the same claims and legal theories on behalf of herself and all absent Class Members.

47. **Adequacy**: Plaintiff is an adequate Class representative because her interests do not materially or irreconcilably conflict with the interests of the Class that she seeks to represent, she has retained counsel competent and highly experienced in complex class action litigation, and they intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and her counsel.

48. **Superiority**: A class action is superior to all other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Defendant's conduct. It would be virtually impossible for members of the Class individually to effectively redress the wrongs done to them. Even if the members of the Class could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties and to the court system presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication,

economy of scale, and comprehensive supervision by a single court. Members of the Class can be readily identified and notified based on, *inter alia*, Defendant's records and databases.

49. **Commonality and Predominance:** The following questions common to all class members predominate over any potential questions affecting individual class members:

a. Whether Defendant had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class Members' PII/PHI from unauthorized access and disclosure;

b. Whether Defendant failed to exercise reasonable care to secure and safeguard Plaintiff's and Class Members' PII/PHI;

c. Whether Defendant breached its duties to protect Plaintiff's and Class members' PII/PHI;

d. Whether Defendant violated the various statutes alleged herein; and

e. Whether Plaintiff and all other members of the Class are entitled to damages and the measure of such damages and relief.

50. Defendant has acted, and refused to act, on grounds generally applicable to the Class, thereby making appropriate final injunctive and equitable relief with respect to the Class as a whole.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf the Nationwide Class or, Alternatively, the Louisiana Class)

51. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

52. Defendant owed a duty to Plaintiff and all other Class members to exercise reasonable care in safeguarding and protecting the PII/PHI in its possession, custody, or control.

53. Defendant knew the risks of collecting and storing Plaintiff's and all other Class members' PII/PHI and the importance of maintaining secure systems. Defendant knew of the many data breaches that targeted healthcare providers in recent years.

54. Given the nature of Defendant's business, the sensitivity and value of the PII/PHI it maintains, and the resources at its disposal, Defendant should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring.

55. Defendant breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to it—including Plaintiff's and Class members' PII/PHI.

56. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

57. But for Defendant's negligent conduct or breach of the above-described duties owed to Plaintiff and Class members, their PII/PHI would not have been compromised.

58. As a result of Defendant's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other Class

members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (v) 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.

COUNT II
NEGLIGENCE PER SE
(On Behalf the Nationwide Class or, Alternatively, the Louisiana Class)

59. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

60. Defendant's duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

61. Defendant's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by business, such as Defendant, of failing to employ reasonable measures to protect and secure PII/PHI.

62. Defendant violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all other Class members' PII/PHI

and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtains and stores, and the foreseeable consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

63. Defendant's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence per se.

64. Plaintiff and Class members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

65. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against.

66. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

67. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Defendant's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA. Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their

PII/PHI, for which there is a well-established national and international market; and/or (v) 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.

COUNT III
UNJUST ENRICHMENT
(On Behalf the Nationwide Class or, Alternatively, the Louisiana Class)

68. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

69. Plaintiff and Class Members have both a legal and equitable interest in their PHI and PII that was collected by, stored by, and maintained by Defendant—thus conferring a benefit upon Defendant—that was ultimately compromised by the Data Breach.

70. Defendant accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. Defendant also benefitted from the receipt of Plaintiff's and Class members' PHI.

71. As a result of Defendant's failure to safeguard and protect Plaintiff's PII and PHI, conduct, Plaintiff and Class members suffered actual damages.

72. Defendant should not be permitted to retain the benefit belonging to Plaintiff and Class members because Defendant failed to adequately implement the data privacy and security procedures for itself that were mandated by federal, state, and local laws and industry standards.

73. Defendant should be compelled to provide for the benefit of Plaintiff and Class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT IV
Breach of Fiduciary Duty
(On Behalf the Nationwide Class or, Alternatively, the Louisiana Class)

74. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

75. Plaintiff and Class members gave MCNA their PII/PHI in confidence—including through their interactions with companies that utilized Defendant's services—believing that MCNA would protect that information. Plaintiff and Class members would not have provided MCNA with this information had they known it would not be adequately protected. MCNA's acceptance and storage of Plaintiff's and Class members' PII/PHI created a fiduciary relationship between MCNA and Plaintiff and Class members. In light of this relationship, MCNA must act primarily for the benefit of individuals that entrusted their PII and PHI to it, which includes safeguarding and protecting Plaintiff's and Class Members' PII/PHI.

76. MCNA has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class members' PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiff's and Class members' PII/PHI that it collected.

77. As a direct and proximate result of MCNA's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of, or imminent threat of, identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in MCNA's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the

impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT V
Breach of Confidence
(On Behalf the Nationwide Class or, Alternatively, the Louisiana Class)

78. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

79. At all times during Plaintiff's and Class members' interactions with Defendant—including through their interactions with companies that utilized Defendant's services—Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class members' PII that Plaintiff and Class members provided to Defendant (including through their interactions with companies that utilized Defendant's services).

80. Defendant's relationship with Plaintiff and Class members was governed by terms and expectations that Plaintiff's and Class members' PII/PHI would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

81. Plaintiff and Class Members provided their PII/PHI to Defendant—including through their interactions with companies that utilized Defendant's services—with the explicit and implicit understandings that Defendant would protect and not permit the PII/PHI to be disseminated to any unauthorized third parties.

82. Plaintiff and Class members provided their PII/PHI to Defendant—including through their interactions with companies that utilized Defendant's services—with the explicit and implicit understandings that Defendant would take precautions to protect that PII from unauthorized disclosure.

83. Defendant voluntarily received in confidence Plaintiff's and Class members' PII/PHI with the understanding that PII/PHI would not be disclosed or disseminated to unauthorized third parties or to the public.

84. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, Plaintiff's and Class members' PII/PHI was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class members' confidence, and without their express permission.

85. As a proximate result of such unauthorized disclosures, Plaintiff and Class members suffered damages.

COUNT VI
Invasion of Privacy
(Intrusion Upon Seclusion)
(On Behalf the Nationwide Class or, Alternatively, the Louisiana Class)

86. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

87. Plaintiff and Class members had a reasonable expectation of privacy in the PII and PHI that Defendant disclosed without authorization.

88. By failing to keep Plaintiff's and Class members' PII and PHI safe and disclosing PHI and PII to unauthorized parties for unauthorized use, Defendant unlawfully invaded Plaintiff's and Class members' privacy by, *inter alia*:

a. intruding into Plaintiff's and class members' private affairs in a manner that would be highly offensive to a reasonable person; and

b. invading Plaintiff's and class members' privacy by improperly using their PHI and PII properly obtained for a specific purpose for another purpose, or disclosing it to some third party;

c. failing to adequately secure their PII and PHI from disclosure to unauthorized persons;

d. enabling the disclosure of Plaintiff's and class members' PII and PHI without consent.

89. Defendant knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiff's and class members' position would consider its actions highly offensive.

90. Defendant knew that its systems and processes for collecting, managing, storing, and protecting PII and PHI entrusted to it were vulnerable to data breaches prior to the Data Breach.

91. Defendant invaded Plaintiff's and Class Members' right to privacy and intruded into Plaintiff's and class members' private affairs by disclosing their PII and PHI to unauthorized persons without their informed, voluntary, affirmative, and clear consent.

92. As a proximate result of such unauthorized disclosures, Plaintiff's and Class members' reasonable expectations of privacy in their PII and PHI was unduly frustrated and thwarted. Defendant's conduct amounted to a serious invasion of Plaintiff's and Class members' protected privacy interests.

93. In failing to protect Plaintiff's and Class members' PII and PHI, and in disclosing that information, Defendant acted with malice and oppression and in conscious disregard of Plaintiff's and class members' rights to have such information kept confidential and private.

94. Plaintiff seeks injunctive relief on behalf of the class, restitution, and all other damages available under this Count.

COUNT VII
DECLARATORY RELIEF
(28 U.S.C. § 2201)
(On Behalf the Nationwide Class or, Alternatively, the Louisiana Class)

95. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

96. An actual controversy has arisen and exists between Plaintiff and members of the Class, on the one hand, and Defendant, on the other hand, concerning the Data Breach and

Defendant's failure to protect Plaintiff's and class members' PHI and PII, including with respect to the issue of whether Defendant took adequate measures to protect that information. Plaintiff and Class members are entitled to judicial determination as to whether Defendant has performed and are adhering to all data privacy obligations as required by law or otherwise to protect Plaintiff's and Class members PHI and PII from unauthorized access, disclosure, and use.

97. A judicial determination of the rights and responsibilities of the parties regarding Defendant's privacy policies and whether they failed to adequately protect PHI and PII is necessary and appropriate to determine with certainty the rights of Plaintiff and the Class members, and so that there is clarity between the parties as to Defendant's data security obligations with respect to PHI and PII going forward, in view of the ongoing relationships between the parties.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of the class members, by and through undersigned counsel, respectfully requests that the Court grant the following relief:

A. Certify this case as a class action pursuant to Fed. R. Civ. P. 23, and appoint Plaintiff as the class representative and undersigned counsel as class counsel;

B. Award Plaintiff and class members actual and statutory damages, punitive damages, and monetary damages to the maximum extent allowable;

C. Award declaratory and injunctive relief as permitted by law or equity to assure that Class members have an effective remedy, including enjoining Defendant from continuing the unlawful practices as set forth above;

D. Award Plaintiff and Class members pre-judgment and post-judgment interest to the maximum extent allowable;

E. Award Plaintiff and Class members reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Award Plaintiff and Class members such other favorable relief as allowable under law or at equity.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: June 16, 2023

Respectfully submitted,

By: */s/ Jon M. Herskowitz, Esq.*

Jon M. Herskowitz, Esq.
Baron & Herskowitz
9100 S. Dadeland Blvd.
Suite 1704
Miami, Florida 33156
Telephone: (305) 670-0101
Facsimile: (305) 670-2393
jon@bhfloridalaw.com
silvia@bhfloridalaw.com

Joseph G. Sauder (*pro hac vice* forthcoming)
Joseph B. Kenney (*pro hac vice* forthcoming)
SAUDER SCHELKOPF LLC
1109 Lancaster Avenue
Berwyn, PA 19312
Telephone: (888) 711-9975
Facsimile: (610) 421-1326
jgs@sstriallawyers.com
jbk@sstriallawyers.com

Attorneys for Plaintiff