

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF SOUTH CAROLINA**

<p>Jennifer Boykin, <i>on behalf of herself and all others similarly situated</i>,</p> <p style="text-align: center;">Plaintiff,</p> <p>v.</p> <p>Choice Health Insurance LLC,</p> <p style="text-align: center;">Defendant.</p>	<p>CASE NO. 4:22-cv-03940-JD</p> <p>FIRST AMENDED CLASS ACTION COMPLAINT</p> <p>JURY TRIAL DEMANDED</p>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------

Plaintiff Jennifer Boykin (“Plaintiff”) brings this First Amended Class Action Complaint against Choice Health Insurance LLC (“Defendant”), individually and on behalf of all others similarly situated (“Class Members”), and alleges, upon personal knowledge as to her own actions and her counsel’s investigations, and upon information and belief as to all other matters, as follows:

1. Defendant is an “independent broker” that offers health insurance to individuals and families throughout the United States.
2. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard personally identifiable information including, but not limited to, Plaintiff’s and Class Members’ name, Social Security number, Medicare beneficiary identification number, date of birth, address and contact information, and health insurance information (collectively, “Private Information” or “PII and PHI”).
3. In order to provide insurance quotes or services, Defendant required Plaintiff and Class Members to provide it with their Private Information. By obtaining, collecting, using, and deriving a benefit from the Private Information of Plaintiff and Class Members, Defendant

assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. By voluntarily undertaking the collection of this sensitive Private Information, Defendant assumed a duty to use due care to protect that information.

4. Despite its duties to Plaintiff and Class Members, Defendant stored their Private Information on a database that was negligently and/or recklessly configured. This misconfiguration allowed files on the database to be accessed without a password or any form of multifactor authentication.

5. On May 7, 2022, an unauthorized individual accessed and exfiltrated Plaintiff's and Class Members' Private Information from the misconfigured database and listed it for sale on the dark web (the "Data Breach").¹

6. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Plaintiff's and Class Members' Private Information that it collected and maintained, and for failing to provide adequate notice to Plaintiff and other Class Members that their information had been stolen by criminals and listed for sale on the dark web.

7. Defendant maintained the Private Information in a reckless and negligent manner. In particular, the Private Information was maintained on a database that was not password protected and therefore accessible to any member of the public. Foreseeably, cybercriminals exploited this obvious vulnerability, exfiltrated Plaintiff's and Class Members' Private Information from the database, and then listed this information for sale on the dark web.

¹ <https://oag.ca.gov/system/files/Choice%20Health%20-%20Template%20Notification%20Letter%20to%20Affected%20Individuals.pdf> (last accessed: October 20, 2022).

8. As a result of the Data Breach, Plaintiff and Class Members suffered ascertainable losses, including but not limited to, a loss of privacy, the loss of the benefit of their bargain, out-of-pocket monetary losses and expenses, the value of their time reasonably incurred to remedy or mitigate the effects of the attack, the diminished value of their Private Information, and the substantial and imminent risk of identity theft. Given the theft of information that is largely static—like Social Security numbers—this risk will remain with Plaintiff and Class Members for the rest of their lives.

9. Upon information and belief, Plaintiff’s and Class Members’ Private Information remains in Defendant’s possession. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe and should be provided injunctive and other equitable relief.

PARTIES

10. Plaintiff Jennifer Boykin is a Citizen of Florida residing in Pensacola, Florida.

11. Defendant Choice Health Insurance, LLC is a corporation organized under the laws of South Carolina, and its United States headquarters and principal place of business are located at 200 Rodeo Dr., Myrtle Beach, SC 29579.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive of interest and costs. The number of class members exceeds 100, many of whom have different citizenship from Defendant.² Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

² See, e.g., <https://www.mhsindiana.com/newsroom/notice-of-data-breach-choice-health.html> (last visited: March 28, 2023).

13. This Court has personal jurisdiction over Defendant because it operates and is headquartered in this District and conducts substantial business in this District.

14. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover, Defendant is based in this District, maintains Plaintiff's and Class Members' Private Information in this District, and has caused harm to Plaintiff and Class Members in this District.

FACTUAL ALLEGATIONS

Background

15. Since 1993, Defendant has served as an "independent broker" offering healthcare options to individuals and families across the United States.³ Defendant sells Medicare products on Humana Insurance's behalf.⁴

16. Defendant also lists health insurance products for Humana, WellCare Health Plans, Anthem BlueCross BlueShield, Mutual of Omaha, HealthCare.gov, UnitedHealthCare, Cigna, and Aetna.⁵

17. In the ordinary course of receiving insurance quotes and/or brokerage services from Defendant, Plaintiff and Class Members were required to provide Defendant with Private Information.

18. Defendant agreed to and undertook legal duties to maintain the Private Information of Plaintiff and Class Members safely, confidentially, and in compliance with all applicable laws.

³ <https://choicehealthins.com/about.html> (last accessed: October 20, 2022).

⁴ <https://healthitsecurity.com/news/humana-discloses-third-party-data-breach-at-choice-health#:~:text=September%2027%2C%202022%20%2D%20Humana%20disclosed,Medicare%20products%20on%20Humana's%20behalf> (last accessed: October 20, 2022).

⁵ <https://choicehealthins.com/index.html> (last accessed: October 20, 2022).

19. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible to protect Plaintiff's and Class Members' Private Information from unauthorized disclosure.

20. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

21. Plaintiff and Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business and health purposes only, and to make only authorized disclosure of this Private Information.

22. Plaintiff and Class Members directly or indirectly entrusted Defendant with sensitive and confidential information, including their Private Information which includes information that is static, meaning it does not change, and can be used to commit myriad financial crimes.

23. Plaintiff and Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand Defendant safeguard their Private Information.

24. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties.

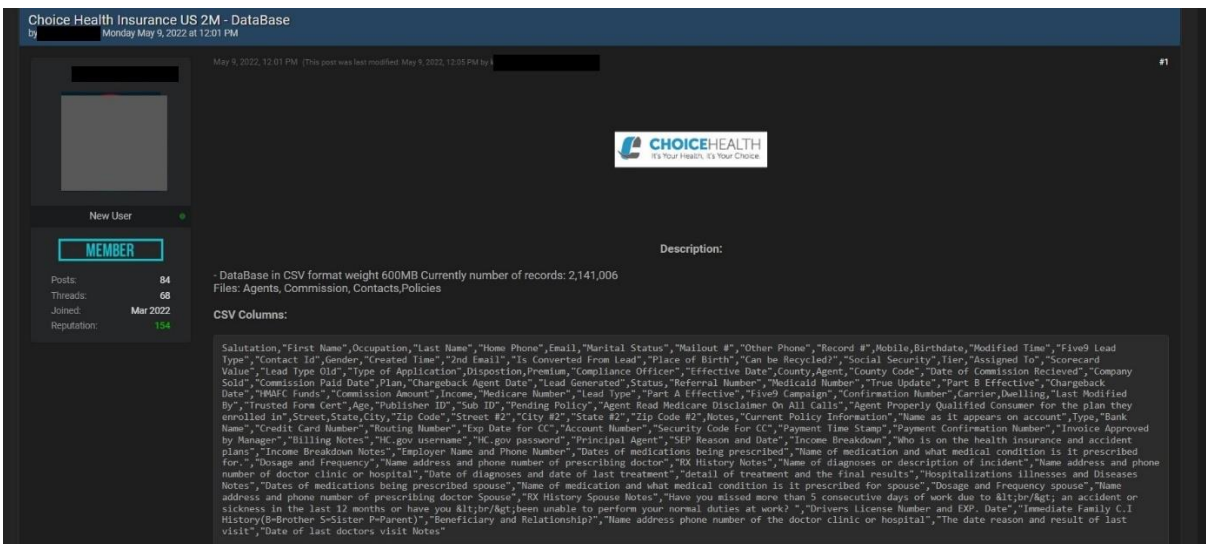
The Data Breach

25. On May 14, 2022, Defendant discovered that information stolen from its database was available for sale on the internet. Specifically, Defendant learned that "an unauthorized person

was offering to make available data taken from [Defendant].”⁶

26. Following a forensic investigation, Defendant discovered that its “database was accessible through the internet due to a security misconfiguration caused by a third-party site provider. The unauthorized party accessed the file and obtained certain files on May 7[, 2022].”⁷ In other words, Defendant’s agent misconfigured one of Defendant’s databases, allowing it to be accessed by members of the public without a password or any form of multifactor authentication. As a result, a criminal was able to exfiltrate this information from the database and place it for sale on the dark web.

27. Indeed, there is evidence of a third party offering to sell Private Information accessed in the Data Breach on the dark web:⁸



(Listing on a popular forum offered data from Choice Health Insurance for sale)

⁶ <https://oag.ca.gov/system/files/Choice%20Health%20-%20Template%20Notification%20Letter%20to%20Affected%20Individuals.pdf> (last accessed: October 20, 2022).

⁷ *Id.*

⁸ <https://www.databreaches.net/choice-health-insurance-notifying-people-after-vendor-error-resulted-in-data-breach/> (last visited: March 28, 2023).

28. Following the Data Breach, Defendant sent notices to Plaintiff and Class Members dated October 7, 2022, stating:

What Happened? On May 14, 2022, Choice Health learned an unauthorized person was offering to make available data allegedly taken from Choice Health. We promptly began an investigation into the incident. On May 18, 2022, we determined that, due to a technical security configuration issue caused by a third-party service provider, a single Choice Health database was accessible through the Internet. Based on our investigation, an unauthorized individual accessed the database from the Internet and obtained certain database files on or about May 7, 2022. We are notifying you of this incident, because your personal information was in the database

What Information Was Involved? The files obtained by the unauthorized individual contained the following types of personal information, some of which may have been included about you: first and last name, Social Security number; Medicare beneficiary identification number; date of birth; address and contact information; and health insurance information.

29. Defendant's Notice of Data Breach admits that Plaintiff's and Class Members' Private Information was accessed without authorization, exfiltrated by cybercriminals, and posted for sale on the internet.⁹ Plaintiff's further investigation shows Plaintiff's and Class Members' Private Information was then posted for sale on the dark web.

30. Defendant admits that cybercriminals not only viewed and accessed Plaintiff's and Class Members' Private Information, but also removed it from Defendant's database and placed it for sale on the dark web.

31. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiff and Class Members, causing the exposure of Private Information. For example, Defendant failed to

⁹ See <https://oag.ca.gov/system/files/Choice%20Health%20-%20Template%20Notification%20Letter%20to%20Affected%20Individuals.pdf> (last visited: March 28, 2023).

implement basic security measures, like password protection or multifactor authentication. Defendant's own notices of the Data Breach stated that Defendant only implemented such measures after the Data Breach. For example, a notice provided to one of Defendant's clients states that:

Upon learning of the incident, Choice Health promptly corrected the security settings on the database and confirmed it is no longer accessible through the Internet. They have also taken steps to enhance their data security measures to prevent the occurrence of a similar event in the future, including requiring multi-factor authentication for all access to database files.¹⁰

32. Because Defendant failed to properly protect safeguard Plaintiff's and Class Members' Private Information, an unauthorized third party was able to access Defendant's database, and then access and exfiltrate Plaintiff's and Class Members' Private Information stored on Defendant's database. This Private Information was then listed for sale on the dark web.

33. While it is a general rule under South Carolina law that a party does not have a duty to protect others from the criminal acts of a third party, the law does find such a duty when the defendant creates a situation that it knew or should have known posed a substantial risk of loss and injury to an identifiable person. Here, Defendant created the risk by failing to properly configure its database, allowing it to be accessed without a password or any form of multi-factor authentication. Defendant knew or should have known this, and as such owed Plaintiff and Class members a duty of due care to protect their Private Information.

34. The unencrypted PII and PHI of Plaintiff and Class Members has already been listed for sale on the internet. In addition, unencrypted PII and PHI may fall into the hands of companies that will use the detailed PII and PHI for targeted marketing without the approval of

¹⁰ <https://www.mhsindiana.com/newsroom/notice-of-data-breach-choice-health.html> (last visited March 28, 2023).

Plaintiff and Class Members. In turn, unauthorized individuals can easily access the PII and PHI of Plaintiff and Class Members.

Plaintiff Jennifer Boykin's Experience

35. Plaintiff is very careful about sharing her sensitive Private Information. Plaintiff has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff stores any documents containing her sensitive PII in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for her various online accounts.

36. Plaintiff entrusted her Private Information to Defendant for the purpose of receiving health insurance quotes. Plaintiff only did so because she believed that Defendant would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

37. Plaintiff received a letter from Defendant dated October 7, 2022 informing her of the Data Breach. This letter stated that:

On May 14, 2022, Choice Health learned an unauthorized person was offering to make available data allegedly taken from Choice Health.... On May 18, 2022, we determined that, due to a technical security configuration issue ..., a single Choice Health database was accessible through the internet. Based on our investigation, an unauthorized individual accessed the database from the internet and obtained certain database files on or about May 7, 2022. We are notifying you because your personal information was in the database.

38. The letter further indicated that Plaintiff's "first and last name, address, provider names, medical history, SSN [Social Security number], email, dates of coverage, health plan id number, Medicaid number, plan information, and Medicare number" may have been included in the files taken from the database.

39. The letter stated that in response, Defendant “reconfigure[d] the security settings on the database” so that it was “no longer accessible through the Internet,” and that it took additional measures to “prevent the occurrence of a similar event,” such as “requiring multi-factor authentication for all access to database files.”

40. Plaintiff suffered injury from a loss of privacy the moment that her Private Information was accessed and exfiltrated by a third party without authorization.

41. Plaintiff has also suffered injury in the form of damages to and diminution in the value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when her Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and later placed for sale on the dark web.

42. The access, exfiltration, and placement of Plaintiff’s Private Information for sale on the dark web has also caused Plaintiff to suffer has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

43. This risk from the Data Breach has caused Plaintiff to spend significant time dealing with issues related to the Data Breach (approximately 15 hours), which includes time spent verifying the legitimacy of the Notice of Data Breach, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant’s direction.

44. Defendant acknowledges the risk posed to Plaintiff and her Private Information. Specifically, the Notice of Data Breach provided specific steps that Plaintiff should consider taking to “protect” herself as a result of the Data Breach, including “reviewing [her] account statements

and credit reports” and being “attentive to documents related to medical services that [Plaintiff] usually receive[s] and that suddenly do not arrive, as [she] usually receive[s] them.”

45. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff to suffer stress, fear, and anxiety.

46. Plaintiff has a continuing interest in ensuring that Plaintiff’s Private Information, which, upon information and belief, remain backed up in Defendant’s possession, is protected, and safeguarded from future breaches.

The Data Breach was Foreseeable

47. As explained by the Federal Bureau of Investigation, “[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection.”¹¹

48. Defendant’s data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry preceding the date of the breach.

49. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020. Of the 1,862 recorded data breaches, 330 of them, or 17.7% were in the medical or healthcare industry.¹² The 330 reported breaches in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.

50. In light of recent high profile cybersecurity incidents at other healthcare partner and

¹¹ See How to Protect Your Networks from RANSOMWARE, at 3, available at <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view> (last accessed Mar. 25, 2023).

¹² See 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at <https://notified.idtheftcenter.org/s/>), at 6.

provider companies, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

51. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation (“FBI”) and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, “[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals... because they often have lesser IT defenses and a high incentive to regain access to their data quickly.”¹³

52. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.¹⁴

53. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant’s industry, including Defendant.

Value of PII and PHI

54. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity

¹³ FBI, Secret Service Warn of Targeted, Law360 (Nov.18,2019), <https://www.law360.com/articles/1220974/fbisecret-service-warn-of-targeted-ransomware>

¹⁴ See Maria Hernandez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), <https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack>.

credentials. For example, personal information can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.¹⁵ Experian reports that a stolen credit or debit card number can sell for \$5 to \$110 on the dark web.¹⁶ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.¹⁷

55. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts.

56. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information...[is] worth more than 10x on the black market.”¹⁸

57. According to account monitoring company LogDog, medical data, such as PHI, sells for \$50 and up on the Dark Web.¹⁹

58. Among other forms of fraud, identity thieves may obtain driver’s licenses,

¹⁵ *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last accessed Mar. 25, 2023).

¹⁶ *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last accessed Mar. 25, 2023).

¹⁷ *In the Dark*, VPNOOverview, 2019, available at: <https://vpnooverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed Mar. 25, 2023).

¹⁸ Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last accessed Mar. 25, 2023).

¹⁹ Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), <https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content> (last accessed Mar. 25, 2023).

government benefits, medical services, and housing or even give false information to police.

59. The fraudulent activity resulting from the Data Breach may not come to light for years.

60. Theft of PHI is also gravely serious: “[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief’s health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected.”

61. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII and PHI on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds’ medical insurance premiums.

62. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.²⁰

63. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII and PHI of Plaintiff and Class Members and the foreseeable consequences that would occur if Defendant’s data security system was breached, including,

²⁰ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf> (last accessed Aug. 23, 2021).

specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

64. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII and PHI.

65. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

66. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII and PHI of Plaintiff and Class Members.

67. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

68. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

69. Plaintiff and the Class Members relied on Defendant to implement and follow adequate data security policies and protocols, to keep their Private Information confidential and securely maintained, to use such Private Information solely for business and health care purposes, and to prevent the unauthorized disclosures of the Private Information.

Defendant Failed to Properly Protect Plaintiff's and Class Members' Private Information

70. Defendant could have prevented this Data Breach by properly securing and encrypting the systems containing the Private Information of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data, especially for individuals with whom it had not had a relationship for a period of time.

71. Defendant's negligence in safeguarding the PII and PHI of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to companies like Defendant to protect and secure sensitive data they possess.

72. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII and PHI of Plaintiff and Class Members from being compromised.

73. To prevent and detect unauthorized cyber-attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted

via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.²¹

74. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

²¹ *Id.* at 3-4.

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

75. Given that Defendant was storing the PII and PHI of Plaintiff and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks. Instead, Defendant failed to implement basic security measures, like password protection, encryption, or multifactor authentication.

Defendant Failed to Comply with FTC Guidelines

76. The Federal Trade Commission (“FTC”) has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making.

77. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network’s vulnerabilities; and implement policies to correct any security problems.²²

78. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords

²² Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

79. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions clarify the measures businesses take to meet their data security obligations.

80. Defendant failed to properly implement basic data security practices, such as making a database storing Private Information available to the public without the use of a password or multifactor authentication.

81. Defendant’s failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff’s and Class Members’ PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

82. Defendant was always fully aware of its obligation to protect the PII and PHI of Plaintiff and Class members. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant failed to Comply with Industry Standards

83. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

84. Several best practices have been identified that at a minimum should be

implemented by service providers like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and antimalware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

85. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

86. The foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

As a Result of Defendant's Failure to Safeguard Private Information, Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft and Have Experienced Substantial Harm.

87. Plaintiff and members of the proposed Class have suffered injury from the access to, and misuse of, their PHI that can be directly traced to Defendant.

88. The ramifications of Defendant's failure to keep Plaintiff's and the Class's PHI secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

89. The FTC defines identity theft as "a fraud committed or attempted using the

identifying information of another person without authority.” 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.”

90. According to experts, one out of four data breach notification recipients become a victim of identity fraud.

91. As a result of Defendant’s failures to prevent—and to timely detect—the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

- a. The loss of the opportunity to control how their PHI is used;
- b. The diminution in value of their PHI;
- c. The compromise and continuing publication of their PHI;
- 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 associated with the time and effort expended 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. Delay in receipt of tax refund monies;
- g. Unauthorized use of stolen PHI; and
- h. The continued risk to their PHI, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PHI in their possession.

92. One such example of criminals using PHI for profit, to the detriment of Plaintiff and the Class Members, is the development of “Fullz” packages.

93. Cyber-criminals can cross-reference two sources of PHI to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as “Fullz” packages.

94. The development of “Fullz” packages means that stolen PHI from the Data Breach can easily be used to link and identify it to Plaintiff’s and the proposed Class’s phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PHI stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff’s and other members of the proposed Class’s stolen PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

95. According to the FBI’s Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than \$3.5 billion in losses to individuals and business victims.

96. Further, according to the same report, “rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good.” Defendant did not rapidly report to Plaintiff and the Class that their PHI had been stolen, and in fact did not notify Plaintiff

for five months.

97. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

98. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their PHI. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

99. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PHI. To protect themselves, Plaintiff and the Class will need to be remain vigilant against unauthorized data use for years or even decades to come.

100. According to the FTC, unauthorized PHI disclosures are extremely damaging to consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout.²³ The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

101. Defendant's failure to properly notify Plaintiff and Class Members of the Data Breach exacerbated Plaintiff's and Class Members' injury by depriving them of the earliest ability

²³ See Taking Charge, What to Do If Your Identity is Stolen, FTC, at 3 (2012), <https://www.ojp.gov/ncjrs/virtual-library/abstracts/taking-charge-what-do-if-your-identity-stolen> (last visited October 10, 2022).

to take appropriate measures to protect their PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

Plaintiff's and Class Members' Damages

102. To date, Defendant has done little to provide Plaintiff and Class Members with relief for the damages they have suffered as a result of the Data Breach, including, but not limited to, the costs and loss of time they incurred because of the Data Breach. Defendant has only offered 24 months of inadequate identity monitoring services, despite Plaintiff and Class Members being at risk of identity theft and fraud for the remainder of their lifetimes.

103. The 24 months of credit monitoring offered to persons whose Private Information was compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud. What's more, Defendant places the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this Data Breach.

104. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

105. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

106. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

107. Plaintiff and Class Members face substantial risk of being targeted for future

phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

108. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

109. Plaintiff and Class Members may also incur out-of-pocket costs for further protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

110. Defendant's delay in noticing affected persons of the theft of their Private Information prevented early mitigation efforts and compounded the harm.

111. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

- a. Reviewing and monitoring financial and other sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;
- b. Purchasing credit monitoring and identity theft prevention;
- c. Placing "freezes" and "alerts" with reporting agencies;
- d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;
- e. Contacting financial institutions and closing or modifying financial accounts; and
- f. Closely reviewing and monitoring Social Security number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to

come.

112. Moreover, Plaintiff and Class Members have an interest in ensuring that their Personal and Medical Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is encrypted and password protected.

113. Defendant acknowledges the harm caused to Plaintiff and Class Members because it offers a complimentary 24-month credit monitoring program via Experian IdentityWorks.²⁴

CLASS ALLEGATIONS

114. Plaintiff brings this nationwide class action on behalf of herself and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

115. The Nationwide Class that Plaintiff seek to represent is defined as follows:

All persons whose Private Information was actually or potentially accessed or acquired during the Data Breach event that is the subject of the Notice of Data Breach that Defendant published to Plaintiff and other Class Members on or around October 7, 2022 (the “Class”).

116. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant’s parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local

²⁴ <https://oag.ca.gov/system/files/Choice%20Health%20-%20Template%20Notification%20Letter%20to%20Affected%20Individuals.pdf> (last visited: March 28, 2023).

governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

117. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

118. Numerosity, Fed R. Civ. P. 23(a)(1): Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are certainly tens of thousands, and possibly in excess of 100,000 individuals whose Private Information was improperly accessed in the Data Breach, and each Class is apparently identifiable within Defendant's records.

119. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

- a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiff and Class Members;
- b. Whether Defendant had duties not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;
- c. Whether Defendant failed to adequately safeguard the Private Information of Plaintiff and Class Members;
- d. Whether and when Defendant actually learned of the Data Breach;
- e. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;
- f. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;
- g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

- h. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- i. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;
- j. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and
- k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

120. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance.

121. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

122. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

123. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

124. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

125. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with

prosecuting this lawsuit as a class action.

126. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

127. Unless a Class-wide injunction is issued, Defendant may continue in their failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

128. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

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

- a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;
- b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;
- c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
- d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;
- e. Whether Defendant breached the implied contract;

- f. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information had been compromised;
- g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- h. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

(On Behalf of Plaintiff and the Putative Nationwide Rule 23 Class)

130. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

131. Plaintiff and the Class entrusted Defendant with their Private Information.

132. Plaintiff and the Class entrusted their Private Information to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their information for business purposes only, and/or not disclose their Private Information to unauthorized third parties.

133. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and the Class could and would suffer if the Private Information were wrongfully disclosed.

134. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Private Information of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

135. By accepting, storing, and maintaining Plaintiff's and Class Members' Private

Information, Defendant undertook a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the Private Information of Plaintiff and the Class Members in Defendant's possession was adequately secured and protected.

136. By accepting, storing, and maintaining Plaintiff's and Class Members' Private Information, Defendant also had a duty to exercise appropriate clearinghouse practices to remove Private Information they were no longer required to retain pursuant to regulations.

137. By accepting, storing, and maintaining Plaintiff's and Class Members' Private Information, Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the Private Information of Plaintiff and the Class.

138. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential Private Information, a necessary part of obtaining services from Defendant.

139. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

140. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

141. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiff and the Class, the critical importance of

providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems.

142. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included their decisions not to comply with industry standards for the safekeeping of the Private Information of Plaintiff and the Class, including basic encryption techniques freely available to Defendant.

143. Defendant knew or should have known that Plaintiff's and Class Members' Private Information was stored on its database and was or should have been aware of the extreme risks associated with failing to properly safeguard Plaintiff's and Class Members' Private Information.

144. Despite being aware of the likelihood that Defendant's databases were vulnerable, not secure, and likely to be attacked by cybercriminals, Defendant failed to correct, update, or upgrade its security protections, thus causing the Data Breach.

145. Plaintiff and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

146. Defendant was in the best position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

147. Defendant had and continue to have a duty to adequately disclose that the Private Information of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Info by third parties.

148. Defendant had a duty to employ proper procedures to prevent the unauthorized

dissemination of the Private Information of Plaintiff and the Class.

149. Defendant has admitted that the Private Information of Plaintiff and Class Members was disclosed due to Defendant's "technical security configuration issue," and thus also accessed and exfiltrated by unauthorized third persons as a result of the Data Breach.

150. Defendant improperly and inadequately safeguarded the Private Information of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

151. Defendant, through its actions and/or omissions, unlawfully breached their duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the Private Information of Plaintiff and the Class during the time the Private Information was within Defendant's possession or control.

152. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the Private Information of Plaintiff and the Class in the face of increased risk of theft.

153. Defendant, through its actions and/or omissions, unlawfully breached their duty to Plaintiff and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of Private Information.

154. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove Private Information they were no longer required to retain pursuant to regulations.

155. Defendant, through its actions and/or omissions, unlawfully breached their duty to adequately and timely disclose to Plaintiff and the Class the existence and scope of the Data Breach.

156. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Nationwide Class, the Private Information of Plaintiff and the Class would not have been compromised.

157. Said differently, if Defendant had properly prevented a "technical security configuration," then the Data Breach would not have occurred and Plaintiff's and Class Members' Private Information would have been appropriately safeguarded.

158. Plaintiff and Class Members suffered an injury when their Private Information was accessed by unknown third parties.

159. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiff and the Class and the harm, and increased risk of imminent harm, suffered by Plaintiff and the Nationwide Class.

160. The Private Information of Plaintiff and Class Members was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

161. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit

reports; (vii) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of Plaintiff and the Class; and (viii) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

162. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

163. Additionally, as a direct and proximate result of Defendant's negligence Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

164. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT II
VIOLATION OF SOUTH CAROLINA STATE DATA BREACH STATUTES
(On behalf of Plaintiff and the Putative Nationwide Rule 23 Class)

165. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

166. Defendant owns, licenses and/or maintains computerized data that includes Plaintiff's and Class Members' Private Information. It acquires this data for its own purposes and

holds that data in a proprietary fashion.

167. As an insurance broker, Defendant “maintains” Plaintiff’s and Class Members’ Private Information as defined in S.C. Code § 39-1-90(B).

168. Defendant’s conduct, as alleged above, violated the data breach statutes of South Carolina, including, S.C. Code § 1-11-490 and/or S.C. Code § 39-1-90 (the “State Data Breach Acts”).

169. Defendant was required, but failed, to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the cyber security incident described herein.

170. The Data Breach constituted a “breach of the security system” within the meaning of the State Data Breach Acts. The information compromised in the Data Breach constituted “personal identifying information” within the meaning of the State Data Breach Acts.

171. The State Data Breach Acts require disclosure of data breaches “in the most expedient time possible and without unreasonable delay....”

172. Defendant violated the State Data Breach Acts by unreasonably delaying disclosure of the Data Breach to Plaintiff and other Class Members, whose Private Information was, or was reasonably believed to have been, acquired by an unauthorized person.

173. Specifically, Defendant learned of the Data Breach on or around May 14, 2022, but waited five months, until on or around October 7, 2022, to notify Plaintiff and Class Members.

174. Upon information and belief, no law enforcement agency instructed Defendant that notification to Plaintiff and Class Members would impede a criminal investigation.

175. As a result of Defendant’s violation of the State Data Breach Acts, Plaintiff and Class Members incurred damages as alleged herein.

176. Plaintiff, individually and on behalf of the Class, seek all remedies available under the State Data Breach Acts, including, but not limited to: (a) actual damages suffered by Class Members as alleged above; (b) statutory damages for Defendant's willful, intentional, and/or reckless conduct; (c) equitable relief; and (d) reasonable attorneys' fees and costs.

COUNT III
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Putative Nationwide Rule 23 Class)

177. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

178. Plaintiff and Class Members were required to provide Defendant with their Private Information to receive health insurance brokerage quotes.

179. By Plaintiff and Class Members requesting health insurance quotes and providing their Private Information, and by Defendant accepting this Private Information and providing health insurance quotes, the parties mutually assented to implied contracts. These implied contracts included an implicit agreement and understanding that (1) Defendant would adequately safeguard Plaintiff's and Class Members' Private Information from foreseeable threats, (2) that Defendant would delete the information of Plaintiff and Class Members once it no longer had a legitimate need; and (3) that Defendant would provide Plaintiff and Class Members with notice within a reasonable amount of time after suffering a data breach.

180. Defendant provided consideration by providing health insurance quotes or promising to consider Plaintiff and Class Members for health insurance, while Plaintiff and Class Members provided consideration by providing valuable property, their Private Information. Defendant benefitted from the receipt of this Private Information by increasing its pool of potential customers, by using it to provide customers with health insurance, and by using this inherently

valuable information for other commercial purposes, like targeted advertising.

181. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

182. Defendant materially breached its implied contracts with Plaintiff and Class Members when it (1) placed their Private Information on a publicly available database that could (and later was) accessed by members of the public on the internet without a password or multi-factor authentication and (2) waited an unreasonably long time to notify them of the Data Breach. It is common sense that Plaintiff and Class Members would not have provided Defendant with their Private Information had they known that Defendant would not implement basic data security measures or that it would wait several months to notify them of a data breach involving their Private Information.

183. Defendant's breaches of contract have caused Plaintiff and Class Members to suffer damages from the lost benefit of their bargain, out of pocket monetary losses and expenses, loss of time, and diminution of the value of their Private Information.

184. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

COUNT IV
BREACH OF FIDUCIARY DUTY
(On behalf of Plaintiff and the Putative Nationwide Rule 23 Class)

185. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

186. In light of the special relationship between Defendant and Plaintiff and Class Members, whereby Defendant became guardian of Plaintiff and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

187. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant's relationship with its patients, in particular, to keep secure their Private Information.

188. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

189. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to encrypt or otherwise protect the integrity of the systems containing Plaintiff and Class Members' Private Information.

190. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

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

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

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class, and appointing Plaintiff and her Counsel to

represent the Class;

- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;
- C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:
 - i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
 - ii. requiring Defendant to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
 - iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;
 - iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;
 - v. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;
 - vi. requiring Defendant to engage independent third-party security

- auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
 - viii. requiring Defendant to audit, test, and train their security personnel regarding any new or modified procedures;
 - ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;
 - x. requiring Defendant to conduct regular database scanning and securing checks;
 - xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;
 - xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
 - xiii. requiring Defendant to implement a system of tests to assess its respective

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

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including, but not limited to, actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

- F. For prejudgment interest on all amounts awarded; and
- G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: March 28, 2023

Respectfully Submitted,

/s/ Glenn V. Ohanesian

Glenn V. Ohanesian

OHANESIAN LAW FIRM

PO Box 2433

Myrtle Beach, SC 29578

843-626-7193

Email: ohanesianlawfirm@cs.com

CHESTNUT CAMBRONNE PA

Philip J. Krzeski*

100 Washington Avenue South, Suite 1700

Minneapolis, MN 55401

Phone: (612) 339-7300

Fax: (612) 336-2940

Email: pkrzeski@chestnutcambronne.com

MARKOVITS, STOCK, & DEMARCO, LLC

Terence R. Coates*

Dylan J. Gould*

Jonathan T. Deters*

119 E. Court St., Ste. 530

Cincinnati, Ohio 45202

Phone: (513) 665-0201

Fax: (513) 665-0219

Email: dgould@msdlegal.com

Email: tcoates@msdlegal.com

Email: jdeters@msdlegal.com

THE LYON LAW FIRM, LLC

Joseph M. Lyon*

2754 Erie Ave.

Cincinnati, OH 45208

Phone: (513) 381-2333

Fax: (513) 766-9011

Email: jlyon@thelyonfirm.com

**Pro Hac Vice*

Counsel for Plaintiff and Putative Class