UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF MISSOURI

STEPHEN TATE, a.k.a. STEVEN TATE, individually and on behalf of all similarly situated persons,

Plaintiffs,

v.

CONCENTRA HEALTH SERVICES, INC.,

Serve:

C T CORPORATION SYSTEM
120 South Central Avenue
Clayton, MO 63105

SELECT MEDICAL HOLDINGS CORPORATION,

Serve:

SELECT MEDICAL HOLDINGS CORPORATION
4714 Gettysburg Road
Mechanicsburg, PA 17055

and

PERRY JOHNSON & ASSOCIATES, INC.,

Serve:

1489 West Warm Springs Road
Suite 110
Henderson, NV 89012

Defendants.

CIVIL ACTION NO. 4:24-cv-293

Jury Trial Demanded

CLASS ACTION COMPLAINT

Plaintiff **STEPHEN TATE, a.k.a. STEVEN TATE** ("Plaintiff"), individually and on behalf of all others similarly situated, bring this action against Defendants **CONCENTRA HEALTH SERVICES, INC.** ("Concentra"); **SELECT MEDICAL HOLDINGS CORPORATION** ("SMC"); and **PERRY JOHNSON & ASSOCIATES, INC** ("PJA") to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendants. Plaintiff makes the following allegations upon information and belief, except as to their own actions, the investigation of Plaintiff counsel, and the facts that are a matter of public record:

NATURE OF THE ACTION

1. Concentra, wholly owned by Select Medical Holdings Corporation, is the nation's leading provider of occupational medicine, urgent care, physical therapy, drug screening, physical exams, and more. As of September 30, 2023, Concentra operated 539 stand-alone occupational health centers and 135 onsite clinics at employer worksites throughout 41 states. Concentra delivers occupational health services, consumer health, and other direct-to-employer care in its occupational health centers, virtually through its telemedicine program, and in its onsite clinics located at the workplaces of employer customers. Concentra's occupational health services include workers' compensation injury and physical rehabilitation care as well as employer services consisting of substance abuse testing, physical exams, clinical testing, and preventive care. Consumer health consists of patient-directed urgent care treatment of injuries and illnesses. Direct-to-employer services consist of the services described above as well as advanced primary care at Concentra's onsite clinics.

2. PJ&A is "a vendor that provides medical transcription services to healthcare organizations across the country, including Concentra." *See*, **Exhibit A**. To facilitate PJ&A's services, Concentra shared the sensitive Private Information of its patients with PJ&A,

3. This class action arises out of a recent targeted cyberattack and data breach ("Data Breach")[1] where unauthorized third-party criminals retrieved and exfiltrated highly sensitive personally identifying information ("PII")[2] and protected health information ("PHI")[3] (collectively, "Private Information") of Plaintiff and the Class Members.

4. Concentra reported that the information compromised includes "full names and one or more of the following data elements: date of birth, address, medical record number, hospital account number, admission diagnosis, and date(s) and time(s) of service. Some individuals may also have had their Social Security number compromised, as well as insurance information and clinical information from medical transcription files, such as laboratory and diagnostic testing results, medications, the name of the treatment facility, and the name of healthcare providers." **C**oncentra Confirms Almost 4 Million Patients Affected by PJ&A Data Breach. The HIPAA Journal. Steve Alder on Jan 31, 2024. Available at: https://www.hipaajournal.com/pja-data-breach/#:~:text=Concentra%2C%20a%20Texas-based%20physical%20and%20occupational%20health%20provider%2C,report%20the%20breach%20to%20OCR%20themselves%2C%20including%20Concentra. (Last visited: 2/22/2024).

5. The Notice of Security Incident stated the following with respect to the types of

[1] *See*, **Exhibit A**: "**Notice of Security Incident"** dated February 8, 2024?

[2] The Federal Trade Commission defines "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." 17 C.F.R. § 248.201(b)(8).

[3] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d et seq., and its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 Protected health information.

information that was taken:

> **What Information Was Involved?**
>
> The types of information related to you that were potentially accessible during the event include your name, address, Social Security number and medical information.

See, **Exhibit A**: Notice of Security Incident.

6. The Data Breach included protected health information ("PHI") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and personally identifiable information ("PII") that Defendants collected and maintained (collectively "Private Information").

7. The PII and PHI of approximately 4,000,000 Concentra patients was taken in the Data Breach. Those patients, which include Plaintiff and Class Members, suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

8. Plaintiff's and Class Members' sensitive personal information—which was entrusted to Defendants for safe keeping —was compromised and unlawfully accessed due to the Data Breach.

9. Defendants owed a non-delegable duty to Plaintiff and Class Members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their Private Information. Yet, Defendants maintained and shared that Private Information in a negligent and/or reckless manner. In particular, Private Information was maintained on computer systems in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendants, and thus Defendants were on notice that failing to take steps necessary to ensure they properly safeguarded Plaintiff's and

Class Members' Private Information from those risks would leave the Private Information in a vulnerable condition.

10. Plaintiff brings this class action lawsuit to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and Class Members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

11. Plaintiff's and Class Members' Private Information was compromised due to Defendants' negligent and/or careless acts and omissions and Defendants' failure to reasonably and adequately protect Plaintiff's and Class Members' Private Information.

12. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendants, and thus Defendants were on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

13. Plaintiff's and Class Members' identities are now at increased risk of identity theft because of Defendant's negligent conduct since the Private Information that Defendants collected and maintained is now in the hands of data thieves.

14. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's

licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

15. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. As a result of the Data Breach, Plaintiff and Class Members face a substantial risk of imminent and certainly impending harm, heightened here by the loss of Social Security numbers, a class of Private Information which is particularly valuable to identity thieves. Plaintiff and Class Members have and will continue to suffer injuries associated with this risk, including but not limited to a loss of time, mitigation expenses, and anxiety over the misuse of their Private Information.

16. This risk is even more pronounced given the extended amount of time that lapsed between when the Data Breach occurred, when Defendants reportedly determined Plaintiff's and Class Members' Private Information was compromised, and when Defendants actually notified Plaintiff and Class Members about the Data Breach.

17. Even those Class Members who have yet to experience identity theft have to spend time responding to the Data Breach and are at an immediate and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach. Plaintiff and Class Members have incurred, and will continue to incur, damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, diminished value of Private Information, loss of privacy, and/or additional damages as described below.

18. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft. In fact, the Notice of Security Incident encourages Plaintiff and the Class Members to "remain vigilant against incidents of identity theft

and fraud by reviewing your account statements, credit reports, and explanation of benefits forms for suspicious activity and to report any suspicious institution." *See*, **Exhibit A**.

19. Plaintiff and Class Members may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

20. Plaintiff seeks to remedy these harms on behalf of Plaintiff's self and all similarly situated individuals whose PII and PHI was accessed during the Data Breach. Accordingly, Plaintiff brings this action against Defendants, seeking redress for Defendants' unlawful conduct and asserting claims for: (i) negligence; (ii) breach of implied contract; (iii) unjust enrichment; and (vi) breach of fiduciary duty.

21. Through these claims, Plaintiff seeks damages in an amount to be proven at trial, including compensatory damages, reimbursement of out-of-pocket costs, as well as injunctive and other equitable relief, including improvements to Defendants' data security systems, policies, and practices, future annual audits, and adequate credit monitoring services funded by Defendants.

PARTIES

22. Plaintiff STEPHEN TATE, a.k.a. STEVEN TATE ("Plaintiff" or "Tate") is, and at all times mentioned herein was, an individual citizen of the State of Missouri residing in Saint Louis County, Missouri. Plaintiff is a patient who received health care services from Concentra and who Concentra contracted with vendor PJA to provide medical transcription services. Plaintiff Tate was sent and received a Breach Notification letter. Defendants obtained and continue to store and maintain Plaintiff's Private Information. Defendants owe Plaintiff a legal duty and obligation to protect his Private Information from unauthorized access and disclosure. Plaintiff's Private Information was compromised and disclosed as a result of Defendants' inadequate data security

practices, which resulted in the Data Breach. Plaintiff obtained healthcare or related services from Concentra. Concentra required Plaintiff to provide his Private Information as a condition of receiving those services. Based on representations made by Concentra, Plaintiff believed Concentra had implemented and maintained reasonable security procedures and practices to protect his Private Information.

23. Defendant CONCENTRA HEALTH SERVICES, INC. ("Concentra") is incorporated in the state of Nevada, with its Principal Office Address located at 4714 Gettysburg Road, Mechanicsburg, PA, 17055-4325. Defendant CONCENTRA HEALTH SERVICES, INC. can be served through its Registered Agent, C T CORPORATION SYSTEM located at 120 South Central Avenue Clayton, MO 63105.

24. Defendant SELECT MEDICAL HOLDINGS CORPORATION is a Delaware corporation with its principal place of business located at 4714 Gettysburg Road, P.O. Box 2034 Mechanicsburg, Pennsylvania. SELECT MEDICAL HOLDINGS CORPORATION wholly owns Concentra. On the New York Secretary of State's Office, Concentra identifies its Principle Executive Office Address as being located at the same address as SELECT MEDICAL HOLDINGS CORPORATION: 4714 Gettysburg Road, Mechanicsburg, PA, 17055. SELECT MEDICAL HOLDINGS CORPORATION has multiple locations in this District.

25. Defendant PERRY JOHNSON & ASSOCIATES, INC. is a Nevada company that provides healthcare-focused information technology services with its principal place of business at 1489 West Warm Springs Road, Suite 110, Henderson, NV 89012.

JURISDICTION AND VENUE

26. The 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 is approximately 4 million, at least one of whom has different citizenship from Defendant. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

27. This Court has personal jurisdiction over Defendants Concentra and Select Medical Holdings Corporation because they availed themselves of the rights and benefits of the State of Missouri by engaging in activities including (i) directly and/or through its parent companies, affiliates, and/or agents providing services to patients throughout the United States and in this judicial district; (ii) conducting substantial business within this District directly and/or through its parent companies, affiliates, and/or agents; and/or (iii) engaging in other persistent courses of conduct and/or deriving substantial revenue from services provided throughout the United States, including this District.

28. The Court has personal jurisdiction over Perry Johnson & Associates, Inc. because Defendant Perry Johnson & Associates, Inc. availed itself of the rights and benefits of the State of Missouri by engaging in activities including (i) directly and/or through its parent companies, affiliates, and/or agents providing services throughout the United States and in this judicial district; (ii) conducting substantial business within this District directly and/or through its parent companies, affiliates, and/or agents; and/or (iii) engaging in other persistent courses of conduct and/or deriving substantial revenue from services provided throughout the United States, including this District.

29. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(2) because this District is a judicial district in which a substantial part of the events or omissions giving rise to the claim occurred, or a substantial part of property that is the subject of the action is situated.

DEFENDANT CONCENTRA'S BUSINESS

30. Concentra delivers occupational health services, consumer health, and other direct-to-employer care in its occupational health centers, virtually through its telemedicine program, and in its onsite clinics located at the workplaces of employer customers. Concentra's occupational health services include workers' compensation injury and physical rehabilitation care as well as employer services consisting of substance abuse testing, physical exams, clinical testing, and preventive care. Consumer health consists of patient-directed urgent care treatment of injuries and illnesses. Direct-to-employer services consist of the services described above as well as advanced primary care at Concentra's onsite clinics.

31. As of September 2023, Concentra operates 539 stand-alone occupational health centers and 135 onsite clinics at employer worksites throughout 41 states.

32. Plaintiff and Class Members are current or former patients of Concentra and entrusted Concentra with their Private Information as a condition of receiving healthcare and related services from Concentra.

33. Select Medical Holdings Corporation's headquarters are located at the same address as Concentra's Principle Executive Offices. Select Medical Holdings Corporation wholly owns Concentra. Upon information and belief, Select Medical Holdings Corporation. Upon information and belief, Select Medical Holdings Corporation controls Concentra.

DEFENDANT PJA's BUSINESS

34. Defendant PJA is a company that provides healthcare-focused transcription services.

35. PJ&A is "a vendor that provides medical transcription services to healthcare organizations across the country, including Concentra." *See*, **Exhibit A**. See also, fn 6. [4] To

[4] https://www.pjats.com/about-pja/ (last visited Nov. 14, 2023).

facilitate PJ&A's services, Concentra shared the sensitive Private Information of its patients with PJ&A,

36. Medical transcription "is the manual processing of voice reports dictated by physicians and other healthcare professionals into text format."[5]

37. In the ordinary course of providing transcription services to customers which are generally healthcare providers, customers provide to PJA access to their patient data, such as: "name, address, Social Security number, medical information (See Exhibit A). Additionally, date of birth, address, medical record number, hospital account number, admission diagnosis, and date(s) and time(s) of service. Some individuals may also have had their Social Security number compromised, as well as insurance information and clinical information from medical transcription files, such as laboratory and diagnostic testing results, medications, the name of the treatment facility, and the name of healthcare providers." [6]

38. Additional sources indicate that PJA's data breach involved patient data, including: Names; Dates of birth; Social Security numbers; Driver's license numbers; Tribal identification numbers; Financial account information; Payment card information; Medical histories; Treatment information; Medication or prescription information; Beneficiary information; Provider information; Address, phone number, and email address, and; Health insurance information.

39. On information and belief, Defendant PJA claims that its medical transcription and

---

[5] *Medical Transcription (MT)*, TechTarget, available at https://www.techtarget.com/searchhealthit/definition/medical-transcription-MT (last visited Nov. 14, 2023).

[6] 1. Concentra Confirms Almost 4 Million Patients Affected by PJ&A Data Breach. The HIPAA Journal. Steve Alder on Jan 31, 2024. Available at: https://www.hipaajournal.com/pja-data-breach/#:~:text=Concentra%2C%20a%20Texas-based%20physical%20and%20occupational%20health%20provider%2C,report%20the%20breach%20to%20OCR%20themselves%2C%20including%20Concentra. (Last visited: 2/22/2024).

reporting products are "HIPAA compliant" and provides each of its customers with a HIPAA compliant Notice of its Privacy Practices (the "Privacy Notice") in respect to how they handle customers' sensitive information.[7]

40. Thus, because PJA certifies that its medical transcription products comply with HIPAA, PJA promises to follow HIPAA's standards for security and privacy of PHI.[8]

41. As a condition of receiving medical transcription services, Defendant PJA requires that its customers entrust it with highly sensitive personal information.

42. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant PJA 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 disclosure.

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

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

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

---

[7] *See Medical Transcription and Reporting*, PJ&A, available at https://www.pjats.com/transcription-reporting/ (last visited Nov. 14, 2023).

[8] *See* 45 C.F.R. § 164 (specifying standards for security and privacy of PHI binding on entities subject to HIPAA).

46. However, Defendants did not maintain adequate security to protect their systems from infiltration by cybercriminals. Contrary to their representations, Defendants failed to implement adequate data security measures, as evidenced by Defendants' admission of the Data Breach, which affected approximately 4 million Concentra patients and several million others.

47. PJ&A waited more than six months after it first became aware of suspicious activity on its systems to notify Concentra "that certain information related to particular Concentra patients was potentially affected by a cybersecurity event."[9]

48. Concentra waited another three months to begin informing patients that their Private Information was affected by the Data Breach. See Exhibit A.

THE CYBERATTACK AND DATA BREACH

49. On May 2, 2023, Defendant PJA became aware of a possible cybersecurity incident affecting its systems. PJA launched an investigation, retaining third-party cybersecurity vendors to assist with the investigation.[10]

50. "On May 2, 2023, PJ&A became aware of suspicious activity on its systems.". See, Exhibit A. In response, "PJ&A launched an investigation, with the assistance of third-party cybersecurity specialists, to determine the nature and scope of the event. The investigation determined that between March 27, 2023 and May 2, 2023, an unauthorized actor gained access to certain PJ&A systems and that information contained within those systems was accessible to the unauthorized actor." *Id*.

51. According to PJ&A, "[t]he investigation also determined that on or about April 7,

[9] U.S. Department of Health and Human Services, *Cases Currently Under Investigation*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Feb. 15, 2024)

[10] *Notice of Data Breach*, PJ&A, available at https://oag.ca.gov/system/files/TemplateNotification.pdf.

2023, and April 19, 2023, the unauthorized actor gained access to a system containing information related to Concentra patients." *Id.*

52. PJA determined that the following types of information potentially compromised from the Data Breach include, but are not limited to: "name, date of birth, address, medical record number, hospital account number, admission diagnosis, [] date(s) and time(s) of service[,] Social Security numbers, information and clinical information from medical transcription files, such as laboratory and diagnostic testing results, medications, the name of the treatment facility, and the name of healthcare providers."[11]

53. Upon information, the Private Information stored and maintained by Defendant PJA was not encrypted.

54. Upon information and belief, the targeted cyberattack was expressly designed to gain access to private and confidential data, including (among other things) the PII and PHI of patients like Plaintiff and the Class Members.

55. Upon information and belief, the cyberattack was targeted at Defendant, due to their status as entities that collect, create, and maintain both PII and PHI.

56. On or about November 3, 2023, PJA published a data breach notification letter on the California Attorney General's website notifying the public of the Data Breach.[12]

57. Upon information and belief, Plaintiff's Private Information was accessed and stolen in the Data Breach.

58. PJA informed impacted patients that they should take steps to monitor accounts "for the next 12 to 24 months" and review statements from healthcare providers for potential

[11] *Id.*
[12] *Search Data Security Breaches*, State of Cal. Dep't of Justice, available at https://oag.ca.gov/privacy/databreach/list (last visited Nov. 15, 2023).

fraudulent charges. [13]

59. Further, PJA offered some impacted patients credit/identity monitoring services.[14]

60. The offer of identity monitoring services is an acknowledgment by PJA that the impacted customers are subject to an imminent threat of identity theft.

61. Despite discovering the Data Breach in May 2023 and acknowledging that data thieves likely accessed Plaintiff's and the Class Members' Private Information, PJA did not begin to notify affected those who were affected by the data security incident until September 29, 2023; however, PJA failed to notify Concentra until November 10, 2023.[15] Concentra waited until January 9, 2024 to filed a notice of data breach with the U.S. Department of Health and Human Services Office for Civil Rights.[16] Concentra and PJA failed to notify affected patients until it issued a written Notice of Security Incident dated February 8, 2024. *See* **Exhibit A**.

62. Concentra reported that the information compromised includes "full names and one or more of the following data elements: date of birth, address, medical record number, hospital account number, admission diagnosis, and date(s) and time(s) of service. Some individuals may also have had their Social Security number compromised, as well as insurance information and clinical information from medical transcription files, such as laboratory and diagnostic testing results, medications, the name of the treatment facility, and the name of healthcare providers." **C**oncentra Confirms Almost 4 Million Patients Affected by PJ&A Data Breach. The HIPAA

---

[13] *Notice of Data Breach*, PJ&A, available at https://oag.ca.gov/system/files/TemplateNotification.pdf.
[14] *Id*.
[15] *See*, Concentra Confirms Patient Information Leaked in Third-Party Data Breach at PJ&A. JD SUPRA, January 29, 2024. (Available at: https://www.jdsupra.com/legalnews/concentra-confirms-patient-information-9485882/#:~:text=On%20January%209%2C%202024%2C%20Concentra%2C%20Inc.%20filed%20a,breach%20at%20Perry%20Johnson%20%26%20Associates%2C%20Inc.%20%28%E2%80%9CPJ%26A%E2%80%9D%29.)
[16] Id.

Journal. Steve Alder on Jan 31, 2024. Available at: https://www.hipaajournal.com/pja-data-breach/#:~:text=Concentra%2C%20a%20Texas-based%20physical%20and%20occupational%20health%20provider%2C,report%20the%20breach%20to%20OCR%20themselves%2C%20including%20Concentra. (Last visited: 2/22/2024).

63. Defendants had obligations created by HIPAA, contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

64. Plaintiff and Class Members provided their Private Information to Defendants and/or their Agents with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

65. Defendants' 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.

66. In light of recent high profile data breaches at other healthcare companies, Defendants knew or should have known that their electronic records would be targeted by cybercriminals.

67. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation 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."[17]

68. 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.

69. Defendants' failure to promptly notify Plaintiff and Class Members that their Private Information was accessed and stolen allowed cybercriminals to monetize, misuse, or disseminate that Private Information before Plaintiff and Class Members could take affirmative steps to protect their sensitive information. As a result, Plaintiff and Class Members will suffer indefinitely from the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated.

70. The accessed data contained Private Information that was accessible, unencrypted, unprotected, and vulnerable for acquisition and/or exfiltration by the unauthorized actor.

Defendants Fail to Comply with FTC Guidelines

71. 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.

72. 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 customer information that they keep; properly dispose of

[17] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), available at https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited October 1, 2023).

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.[18] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[19]

73. 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 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.

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

75. These FTC enforcement actions include actions against healthcare providers and business associates thereof like Defendant. *See, e.g., In the Matter of Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he

[18] *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 (last visited Jan. 5, 2023).
[19] *Id.*

Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.")

76. Defendants failed to properly implement basic data security practices. Defendants failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

77. Defendants were at all times fully aware of its obligation to protect the PII and PHI of patients. Defendants were also aware of the significant repercussions that would result from its failure to do so.

Defendants Failed to Comply with Industry Standards

78. 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.

79. Several best practices have been identified that a minimum should be implemented by healthcare providers like Defendants, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

80. A number of industry and national best practices have been published and should be used as a go-to resource when developing an institution's cybersecurity standards. The Center for Internet Security (CIS) released its Critical Security Controls, and all healthcare institutions are strongly advised to follow these actions. The CIS Benchmarks are the overwhelming option of choice for auditors worldwide when advising organizations on the adoption of a secure build

standard for any governance and security initiative, including PCI DSS, HIPAA, NIST 800-53, SOX, FISMA, ISO/IEC 27002, Graham Leach Bliley and ITIL.[20]

81. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

82. Upon information and belief, Defendants failed to meet the minimum standards of the following cybersecurity 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 established standards in reasonable cybersecurity readiness.

Defendants' Conduct Violates HIPAA and Evidences Their Insufficient Data Security

83. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

84. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

85. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the

[20] *See CIS Benchmarks FAQ*, Center for Internet Security, available at https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq/ (last visited Jan. 5, 2023).

Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendants left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

86. Defendants' Data Breach resulted from a combination of insufficiencies that demonstrate they failed to comply with safeguards mandated by HIPAA regulations.

DEFENDANT'S DUTY TO PLAINTIFF AND CLASS MEMBERS

87. Defendants breached their obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems and data. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor their own data security systems for existing intrusions;

d. Failing to ensure that their vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to train their employees in the proper handling of PII and PHI;

f. Failing to ensure the confidentiality and integrity of electronic PHI they created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

g. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or

software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

h. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

i. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

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

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

l. Failing to ensure compliance with HIPAA security standard rules by their workforces in violation of 45 C.F.R. § 164.306(a)(4);

m. Failing to train all members of their workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

n. Failing to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as they had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304's

definition of "encryption");

o. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act, and;

p. Failing to adhere to industry standards for cybersecurity.

88. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Defendants.

THE CONSEQUENCES OF DEFENDANT'S FAILURES

89. Cyberattacks and data breaches on medical facilities and technology vendors PJA are problematic because of the increased risk of fraud and identity theft.

90. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[21]

91. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims and take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim.

[21] *See* U.S. Gov. Accounting Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (2007), available at https://www.gao.gov/new.items/d07737.pdf (last visited Jan. 5, 2023).

92. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[22]

93. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

94. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, 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.

95. Moreover, theft of Private Information is also gravely serious. PII/PHI is a valuable property right.[23]

96. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious

---

[22] *See IdentityTheft.gov*, Federal Trade Commission, available at https://www.identitytheft.gov/Steps (last visited January 5, 2023).

[23] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

97. Theft of PHI, in particular, is 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."[24]

98. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII/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.

99. It must also be noted there may be a substantial time lag – measured in years – between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

100. According to the U.S. Government Accountability Office, 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.

See GAO Report, at p. 29.

101. Private Information is such a valuable commodity to identity thieves that once the

[24] *See* Federal Trade Commission, *Medical Identity Theft*, available at http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited Jan. 5, 2023).

information has been compromised, criminals often trade the information on the "cyber black-market" for years.

102. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

103. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

104. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[25] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

105. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[26] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[27] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an

[25] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), available at https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.
[26] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1, available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Jan. 5, 2023).
[27] *Id* at 4.

individual's authentic tax return is rejected.

106. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[28]

107. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[29]

108. Medical information is especially valuable to identity thieves.

109. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016 – the same as a Facebook account.[30] That pales in comparison with the asking price for medical data, which was selling for $50 and up.[31]

110. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

---

[28] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), available at http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

[29] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), available at http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[30] *See* Omri Toppol, *Email Security: How You Are Doing It Wrong & Paying Too Much*, LogDog (Feb. 14, 2016), available at https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong/.

[31] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), available at https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content.

111. For this reason, Defendants knew or should have known about these dangers and strengthened their data and email handling systems accordingly. Defendants were put on notice of the substantial and foreseeable risk of harm from a data breach, yet they failed to properly prepare for that risk.

Plaintiff's and Class Members' Damages

112. Given the sensitivity of the Private Information involved in this Data Breach, Plaintiff and Class Members have all suffered damages and will face a substantial risk of additional injuries for years to come, if not the rest of their lives. Defendants have done nothing to compensate Plaintiff or Class Members for many of the injuries they have already suffered. Defendants have not demonstrated any efforts to prevent additional harm from befalling Plaintiff and Class Members as a result of the Data Breach.

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

114. Plaintiff's and Class Members' demographic information, dates of birth, and Social Security numbers were all compromised in the Data Breach and are now in the hands of the cybercriminals.

115. Since being notified of the Data Breach, Plaintiff has spent time dealing with the impact of the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation.

116. Due to the Data Breach, Plaintiff anticipates spending considerable

time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. This includes changing passwords, monitoring his insurance and health accounts for suspicious and/or fraudulent activity, communicating with lawyers.

117. Plaintiff's PII and PHI was compromised as a direct and proximate result of the Data Breach.

118. 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.

119. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

120. 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.

121. 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 target such schemes more effectively to Plaintiff and Class Members.

122. Since the Data Breach, Plaintiff Colon has already been notified by credit monitoring services that his information was detected on the "dark web."

123. 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.

124. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

125. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts and records for misuse. Indeed, Defendant's own notice of data breach provides instructions to Plaintiff and Class Members about all the time that they will need to spend monitor their own accounts, or to establish a security freeze on their credit report.

126. 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. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled, and;

k. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

127. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendants, 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 personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

128. Further, as a result of Defendants' conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life, including what ailments they suffer, whether physical or mental—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

129. As a direct and proximate result of Defendants' actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and are at an imminent and increased risk of future harm.

PLAINTIFF'S EXPERIENCE

130. Plaintiff was a patient of the Defendant Concentra and was required to and did provide Defendants with his Private Information, which it maintained in its systems. Based on representations made by Defendant Concentra, Plaintiff believed Defendant Concentra had implemented and maintained reasonable security procedures and practices to protect his Private

Information.

131. Plaintiff used his debit card to pay for Concentra's services on or about April 7, 2023.

132. Plaintiff received a letter from Defendant PJA dated February 8, 2024 informing him of the Data Breach that occurred previously. *See* **Exhibit A**.

133. As a result, he has taken multiple steps to avoid identity theft, including increasingly carefully reviewing his accounts and contacting counsel.

134. Plaintiff is very careful about sharing sensitive Private Information. He stores any documents containing Private Information in a safe and secure location. He will shred and/or burn documents containing PII or PHI before disposing of those private documents.

135. Plaintiff has not knowingly transmitted unencrypted sensitive Private Information over the Internet. Plaintiff would not have entrusted his Private Information to Defendants had he known of their lax data security policies.

136. As a direct and proximate result of the Data Breach, Plaintiff has made reasonable efforts to mitigate the impact of the Data Breach, including by monitoring his accounts and considering paying out-of-pocket for additional services and is additionally considering enrolling in the credit monitoring service offered by Defendant PJA, and is regularly and closely monitoring his financial accounts.

137. Plaintiff will be forced to spend additional time monitoring his Private Information and has already spent time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities.

138. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the

harms caused by the Data Breach. He faces a present and continuing risk of fraud and identity theft for his lifetime.

139. Plaintiff greatly values his privacy and would not have provided Private Information and/or undertaken the services and paid the amounts that he did if he had known that his Private Information would be maintained using inadequate data security systems.

140. Although Plaintiff appreciates the offer of one year of monitoring, Plaintiff believes that monitoring should be for a significantly longer period of time and is another basis for his damages.

CLASS ALLEGATIONS

141. Plaintiff brings this Action as a class action under Federal Rule of Civil Procedure 23 and seeks certification of the following nationwide Class ("Class"):

> All persons whose personal information was accessed, compromised, copied, stolen, and/or revealed as a result of Defendants' Data Breach.

142. Excluded from the Classes are Defendants, their subsidiaries and affiliates, their officers, directors, the members of their immediate families, and any entity in which Defendants have a controlling interest, to include the legal representatives, heirs, successors, or assigns of any such excluded party. Also excluded are the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

143. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

144. Class certification of Plaintiff's claims is appropriate because Plaintiff can prove the elements of the claims on a class-wide basis utilizing the same evidence as would be used to prove those elements in separate actions alleging the same claims.

145. **Numerosity—Federal Rule of Civil Procedure 23(a)(1)**. The Members of the Class are so numerous that joinder of all Class Members would be impracticable. Upon information and belief, the Class numbers approximately 4 million. Also, the Class is comprised of an easily ascertainable set of patients who were impacted by the Data Breach. The exact number of Class Members can be confirmed through discovery, which includes Defendant's records. The resolution of Plaintiff's and Class Members' claims through a class action will behoove the Parties and this Court.

146. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3)**. Common questions of fact and law exist as to all Members of the Class and predominate over questions affecting only individual Class Members. These common questions of law or fact, include, among other things:

a. Whether Defendants' cybersecurity systems and/or protocols before and during the Data Breach complied with relevant data security laws and industry standards;

b. Whether Defendants properly implemented their purported security measures to safeguard Plaintiff's and Class Members' private information from unauthorized access, propagation, and misuse;

c. Whether Defendants took reasonable measures to determine the extent of the Data Breach after they first discovered the same;

d. Whether Defendants disclosed Plaintiff's and Class Members' private information in contravention of the understanding that the information was being revealed in confidence and should be maintained;

e. Whether Defendants willfully, recklessly, or negligently failed to maintain and execute reasonable procedures and security controls to preclude unauthorized access to Plaintiff's

and the Class Members' private information;

f. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;

g. Whether Defendants had a special duty to Plaintiff and the Class Members;

h. Whether Defendants should have discovered the Data Breach sooner;

i. Whether Defendants failed to provide notice of the Data Breach in a timely manner, and;

j. Whether Defendants were unjustly enriched by their actions;

k. Whether Plaintiff and Class Members are entitled to damages, injunctive relief, or other equitable relief, and the extent of such damages and relief;

147. Defendants engaged in a common course of conduct granting rise to the legal rights sought to be enforced by Plaintiff, on behalf of Plaintiff's self and other Members of the Class. Similar or identical common law violations, business practices, and injuries are involved.

148. **Typicality—Federal Rule of Civil Procedure 23(a)(3)**. Plaintiff's claims are typical of the claims of the other Members of the Class because, *inter alia*, all Class Members were similarly injured and sustained similar monetary and economic injuries as a result of Defendants' misconduct described herein and were accordingly subject to the alleged Data Breach. Also, there are no defenses available to Defendants that are unique to Plaintiff.

149. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4)**. Plaintiff is an adequate representative of the Class because Plaintiff's interests do not conflict with the interests of the Class she seeks to represent, they retained counsel competent and experienced in complex class action litigation, and they will prosecute this action earnestly. The Class's

interests will be fairly and adequately protected by Plaintiff and Plaintiff's counsel.

150. **Injunctive Relief—Federal Rule of Civil Procedure 23(b)(2)**. Defendants acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate regarding the Class under Federal Rule of Civil Procedure 23(b)(2).

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

152. Class certification is also appropriate under Rules 23(b)(1) and/or (b)(2) because:

a. The prosecution of separate actions by the individual Class Members would create a risk of inconsistent or varying adjudications establishing conflicting standards of conduct for Defendants;

b. The prosecution of separate actions by individual Class Members would create a risk of adjudication that would be dispositive of the interests of other Class Members not parties to the adjudications, or would substantially impair or impede their ability to protect their interests;

and

c. Defendants have acted and refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief regarding the Members of the Class as a whole.

153. Class certification is also appropriate because this Court can designate specific claims or issues or class-wise treatment and may designate multiple subclasses under Federal Rule of Civil Procedure 23(c)(4).

154. No unusual difficulties are likely to be encountered in the management of this action as a class action.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

155. Plaintiff re-alleges and incorporate by reference each of the foregoing allegations above as if fully set forth herein.

156. In order to receive medical treatments and services, customers of Defendants required Plaintiff and Class Members to submit non-public Private Information, such as PII and PHI.

157. Plaintiff and Class Members entrusted their Private Information to Defendants with the understanding that Defendants would safeguard their information.

158. By collecting and storing this data in its computer property, and sharing it and using it for commercial gain, Defendants had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendants'

duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

159. Defendants owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

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

161. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1).

162. Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

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

164. Defendants' duty to use reasonable care in protecting confidential data arose not

only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Private Information.

165. Defendants breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failure to periodically ensure that its network system had plans in place to maintain reasonable data security safeguards;

d. Failing to adequately train its employees to recognize and contain phishing attacks;

e. Allowing unauthorized access to Class Members' Private Information;

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

g. Failing to timely notify Class Members about the Data Breach regarding what type of Private Information had been compromised so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

h. Failing to have mitigation and back-up plans in place in the event of a cyber-attack and data breach.

166. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach

of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the medical industry.

167. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

168. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Cyber-Attack and data breach.

169. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit and identity monitoring to all Class Members.

170. Further, pursuant to HIPAA (42 U.S.C. § 1302d et seq.), the FTCA, and the laws of the various states, Defendants were required by law to maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiff's and Class Members' Personal Information.

171. Plaintiff and Class Members are within the class of persons that the HIPAA was intended to protect.

172. The harm that occurred as a result of the Data Breach is the type of harm that HIPAA was intended to guard against. The Federal Health and Human Services' Office for Civil Rights ("OCR") has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures relating to protected health information, caused the same harm as that suffered by Plaintiff and the Class.

173. Plaintiff and Class Members are within the class of persons that the FTCA was intended to protect.

174. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

175. Defendants breached its duties by failing to employ industry standard data and cybersecurity measures to gain compliance with those laws, including, but not limited to, proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

176. It was reasonably foreseeable, particularly given the growing number of data breaches of health information, that the failure to reasonably protect and secure Plaintiff's and Class Members' Personal Information in compliance with applicable laws would result in an unauthorized third-party gaining access to Defendants' networks and computers that stored or contained Plaintiff's and Class Members' Personal Information.

177. Plaintiff's and Class Members' Personal Information constitutes personal property that was stolen due to Defendants' negligence, resulting in harm, injury and damages to Plaintiff and Class Members.

178. Defendants' conduct in violation of applicable laws directly and proximately caused the unauthorized access and disclosure of Plaintiff's and Class Members' unencrypted Personal Information and Plaintiff and Class Members have suffered and will continue to suffer damages as a result of Defendants' conduct. Plaintiff and Class Members seek damages and other relief as a result of Defendants' negligence.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

179. Plaintiff re-alleges and incorporate by reference each of the foregoing allegations above as if fully set forth herein.

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

181. Specifically, Plaintiff entered into a valid and enforceable implied contract with Defendants when they first went for medical care and treatment at one of Defendants' customers' facilities.

182. The valid and enforceable implied contracts to provide medical health care services that Plaintiff and Class Members entered into with Defendants and/or its Agents include the promise to protect non-public Private Information given to Defendants or that Defendants creates on its own from disclosure.

183. When Plaintiff and Class Members provided their Private Information to Defendants and/or its Agents in exchange for medical services, they entered into implied contracts with Defendants pursuant to which Defendants agreed to reasonably protect such information.

184. Defendants and/or its Agents solicited and invited Class Members to provide their Private Information as part of Defendants' regular business practices. Plaintiff and Class Members accepted Defendants' offers and provided their Private Information to Defendants.

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

186. Class Members who paid money to Defendants reasonably believed and expected

that Defendants would use part of those funds to obtain adequate data security. Defendants failed to do so.

187. Under the implied contracts, Defendants and/or its Agents promised and were obligated to: (a) provide healthcare to Plaintiff and Class Members; and (b) protect Plaintiff's and the Class Members' PII/PHI: (i) provided to obtain such health care; and/or (ii) created as a result of providing such health care. In exchange, Plaintiff and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

188. Both the provision of medical services healthcare and the protection of Plaintiff's and Class Members' Private Information were material aspects of these implied contracts.

189. The implied contracts for the provision of medical services – contracts that include the contractual obligations to maintain the privacy of Plaintiff's and Class Members' Private Information—are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendants' privacy policies.

190. Defendant's express representation memorialize and embody the implied contractual obligation requiring Defendants to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

191. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining healthcare private. To patients such as Plaintiff and Class Members, healthcare that does not adhere to industry standard data security protocols to protect Private Information is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security. Plaintiff and Class Members would not have entrusted their Private Information to Defendants and/or its Agents and entered into these implied contracts with Defendants without an understanding that their Private Information would

be safeguarded and protected or entrusted their Private Information to Defendants in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

192. A meeting of the minds occurred, as Plaintiff and Members of the Class agreed to and did provide their Private Information to Defendants and/or its Agents, and paid for the provided healthcare in exchange for, amongst other things, both the provision of health care and medical services and the protection of their Private Information.

193. Plaintiff and Class Members performed their obligations under the contract when they paid for their health care services and provided their Private Information.

194. Defendants materially breached its contractual obligation to protect the non-public Private Information Defendants gathered when the sensitive information was accessed by unauthorized personnel as part of the Data Breach.

195. Defendants materially breached the terms of the implied contracts. Defendants did not maintain the privacy of Plaintiff's and Class Members' Private Information as evidenced by its notifications of the Data Breach to Plaintiff and approximately nine million Class Members. Specifically, Defendants did not comply with industry standards, standards of conduct embodied in statutes like HIPAA and Section 5 of the FTCA, or otherwise protect Plaintiff's and the Class Members' Private Information, as set forth above.

196. The Data Breach was a reasonably foreseeable consequence of Defendants' actions in breach of these contracts.

197. As a result of Defendants' failure to fulfill the data security protections promised in these contracts, Plaintiff and Members of the Class did not receive the full benefit of the bargain, and instead received health care and other medical services that were of a diminished value to that

described in the contracts. Plaintiff and Class Members therefore were damaged in an amount at least equal to the difference in the value of the healthcare with data security protection they paid for and the health care they received.

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

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

200. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

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

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Classes)

202. Plaintiff re-alleges and incorporates by reference each of the foregoing allegations as if fully set forth herein.

203. This count is plead in the alternative to the breach of contract counts above.

204. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendants and/or its Agents and in so doing provided Defendants with their Private Information. In exchange, Plaintiff and Class Members should have received from Defendants the goods and services that were the subject of the transaction and have their Private Information protected with adequate data security.

205. Defendants knew that Plaintiff and Class Members conferred a benefit which Defendants accepted. Defendants profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

206. The amount Plaintiff and Class Members paid for goods and services were used, in part, to pay for use of Defendant's network and the administrative costs of data management and security.

207. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendants failed to implement appropriate data management and security measures that are mandated by industry standards.

208. Defendants failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

209. Defendants acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

210. If Plaintiff and Class Members knew that Defendants had not reasonably secured their Private Information, they would not have agreed to Defendants' services.

211. Plaintiff and Class Members have no adequate remedy at law.

212. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their Private Information is used; (c) the compromise, publication, and/or theft of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (e) lost opportunity costs associated with efforts 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; (f) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (g) future costs in terms of time, effort, and money that 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 Class Members.

213. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

214. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

COUNT IV
BREACH OF CONFIDENCE
(On Behalf of Plaintiff and the Classes)

215. Plaintiff re-alleges and incorporates by reference each of the foregoing allegations as if fully set forth herein.

216. At all times during Plaintiff's and Class Members' interactions with Defendants and/or its Agents, Defendants were fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' Private Information.

217. As alleged herein and above, Defendant's relationship with Plaintiff and Class Members was governed by terms and expectations that Plaintiff's and Class Members' Private Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

218. Plaintiff and Class Members provided their Private Information to Defendants and/or its Agents with the explicit and implicit understandings that Defendants would protect and not permit the Private Information to be disseminated to any unauthorized parties.

219. Plaintiff and Class Members also provided their Private Information to Defendants and/or its Agents with the explicit and implicit understandings that Defendants would take precautions to protect such Private Information from unauthorized disclosure.

220. Defendants voluntarily received in confidence Plaintiff's and Class Members' Private Information with the understanding that the Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

221. Due to Defendant's failure to prevent, detect, or avoid the Data Breach from occurring by, inter alia, following industry standard information security practices to secure Plaintiff's and Class Members' Private Information, Plaintiff's and Class Members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

222. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class Members have suffered damages.

223. But for Defendant's disclosure of Plaintiff's and Class Members' Private Information in violation of the parties' understanding of confidence, their protected Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' protected Private Information, as well as the resulting damages.

224. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' Private Information.

225. As a direct and proximate result of Defendant's breach of confidence, 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, tax fraud, and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended 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 medical fraud, financial fraud and identity theft; (v) 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 Defendants fail to undertake appropriate and adequate measures to protect the Private Information of patients in their continued possession; and (viii) future costs in terms of time,

effort, and money that 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 Class Members.

226. As a direct and proximate result of Defendant's breach of confidence, Plaintiff and Class Members have suffered and will continue to suffer injury and/or harm.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of Plaintiff's self and the Class described above, seeks the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Nationwide Class requested herein;

b. Judgment in favor of Plaintiff and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing Defendants to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members;

e. An order requiring Defendants to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiff and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury of all claims so triable.

DATED: February 26, 2024

Respectfully submitted,

By: /s/ Tiffany Marko Yiatras
Tiffany Marko Yiatras, #58197MO
Francis J. "Casey" Flynn, Jr., #52358MO
CONSUMER PROTECTION LEGAL, LLC
308 Hutchinson Road
Ellisville, Missouri 63011-2029
Tele: 314-541-0317
Email: tiffany@consumerprotectionlegal.com
Email: casey@consumerprotectionlegal.com

ATTORNEYS FOR PLAINTIFF AND THE PROPOSED CLASS

ClassAction.org