UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
TACOMA DIVISION

DONNA BRIM, KIMBERLY PERRY, and JANET TURNER LAMONICA, individually and on behalf of all others similarly situated, Plaintiffs, v. PRESTIGE CARE, INC., Defendant.	Case No. 3:24-cv-05133-BHS **CONSOLIDATED AMENEDED CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

1. Plaintiffs Donna Brim, Kimberly Perry, and Janet Turner Lamonica ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this action against Defendant Prestige Care, Inc. ("Prestige Care" or "Defendant") to obtain damages, restitution, and injunctive relief from Defendant. Plaintiffs make the following allegations upon personal knowledge, information and belief, the investigation of their counsel, and facts that are a matter of public record.

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

NATURE OF THE ACTION

2. Defendant Prestige Care provides senior assisted living and/or employment to individuals, including Plaintiffs and Class Members. This class action arises out of Defendant's failures to properly secure, safeguard, encrypt, and/or timely and adequately destroy Plaintiffs' and Class Members' sensitive personal identifiable information that it had acquired and stored for its business purposes. This failure to secure and monitor its network resulted in a September 2023 data breach ("Data Breach" OR "Breach") of highly sensitive documents and information stored on Prestige Care's computer network.

3. Defendant's data security failures allowed a targeted cyberattack in or about September 2023 to compromise Defendant's network (the "Data Breach") that contained personally identifiable information ("PII") and protected health information ("PHI") (collectively, "the Private Information") of Plaintiffs and other individuals.

4. According to a notice Prestige Care sent to the State Attorney Generals on or about January 31, 2024, 38,087 individuals were affected by the Data Breach.[1]

5. According to a notice on its website, Defendant confirmed that a "data event" occurred on its network on September 7, 2023.

6. Defendant's website notice states: "Through our investigation, we determined that an unauthorized actor may have had access to certain systems that stored personal and health information on September 7, 2023. Prestige Care is undertaking an extensive and time intensive review of what information was potentially impacted and to whom that information relates. On December 18, 2023, Prestige Care determined that information related to certain current former employees and residents was present in its systems. Although Prestige Care has no evidence of

[1] https://apps.web.maine.gov/online/aeviewer/ME/40/d71b6f68-8cda-420e-a064-64a3ae3dc47c.shtml (last accessed Feb. 21, 2024).

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

any identity theft or fraud in connection with this incident, Prestige Care began providing notice to those individuals whose information was impacted."[2]

7. Despite learning of the Data Breach on or about September 7, 2023, and determining that Private Information was involved in the Breach, Defendant did not begin sending notices of the Data Breach (the "Notice of Data Breach Letter") until January 31, 2024, over five months later.

8. The Private Information compromised in the Data Breach included certain personal or protected health information of current and former employees and patients, including Plaintiffs. This Private Information included, but is not limited to names, Social Security numbers, driver's license numbers and/or state identification numbers, financial account information, health insurance information, medical information, email or username and passwords, dates of birth, passport numbers, taxpayer identification numbers, employer identification numbers, employer assigned identification numbers, and military identification numbers.[3]

9. The Private Information was compromised in what Prestige Care refers to as a "data event" in which it "became aware of suspicious activity on our computer network."

10. The cybercriminals intentionally targeted Prestige Care for the highly sensitive Private Information it stores on its computer network, attacked the insufficiently secured network, then exfiltrated highly sensitive PII and PHI, including, but not limited to, Social Security numbers. As a result, the Private Information of Plaintiffs and Class remains in the hands of those cyber-criminals.

11. On information and belief, the cybercriminals responsible for the Breach specifically targeted Defendant and the Private Information of Plaintiffs and Class Members for the purpose

[2] https://www.prestigecare.com/notice-of-data-event/ (last accessed Feb. 21, 2024).

[3] *Id.*

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

of generating a profit from the sale and use of said Private Information, including by committing identity theft and fraud and other criminal acts.

12. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect individuals' Private Information, with which it was entrusted for either senior assisted living and care or employment or both. Had Defendant implemented adequate safeguards, reasonable cyber-security procedures, and protocols necessary to protect the Private Information of Plaintiffs and Class Members, the Data Breach would not have occurred or its effects would have been mitigated.

13. On information and belief, Defendant was able to implement reasonable safeguards that would have prevented the Data Breach or mitigated its affects, but failed to do so.

14. Plaintiffs bring this class action lawsuit on behalf of themselves and all others similarly situated 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 Plaintiffs and other Class Members that their information had been subject to unauthorized access by an unknown, third party.

15. Defendant maintained the Private Information in a reckless manner. In particular, Private Information was maintained on Defendant Prestige Care's computer network in a condition vulnerable to cyberattacks. On information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

16. Defendant disregarded the rights of Plaintiffs and Class Members by, inter alia, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiffs' and Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiffs and Class Members with prompt and full notice of the Data Breach.

17. Defendant Prestige Care failed to properly monitor the computer network and systems that housed the Private Information. Had Prestige Care properly monitored its computer network and systems, it would have discovered the intrusion sooner rather than allowing cybercriminals almost a month of unimpeded access to the Private Information of Plaintiffs and Class Members.

18. Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct. The Private Information that Defendant Prestige Care collected and maintained is now in the hands of data thieves.

19. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, for example, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, filing false medical claims 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.

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

20. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class Members must now and for years into the future closely monitor their financial accounts to guard against identity theft.

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

22. Plaintiffs and Class Members have suffered injuries as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time (that Plaintiffs and Class Members could have dedicated to employment and recreation) and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) misuse of their Private Information; (vi) loss of benefit of the bargain; (vii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up 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.

23. Through this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach (the "Class").

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

24. Accordingly, Plaintiffs bring this action against Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence, (ii) breach of implied contract, (iii) breach of fiduciary duty, (iv) unjust enrichment, (v) declaratory relief, and (vi) violations of Washington Consumer Protection Act, RCW 19.86.

25. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, as well as long-term and adequate credit monitoring services funded by Defendant, and declaratory relief.

PARTIES

26. Plaintiff Donna Brim is a natural person, resident, and citizen of the State of Oregon. Plaintiff Brim received notice of the Data Breach dated January 31, 2024.

27. Plaintiff Kimberly Perry is a natural person, resident, and citizen of the State of Oregon. Plaintiff Perry received notice of the Data Breach dated January 31, 2024.

28. Plaintiff Janet Turner Lamonica is a natural person, resident, and citizen of the State of Oregon. Plaintiff Turner Lamonica received notice of the Data Breach dated January 31, 2024.

29. Prestige Care, Inc. is a Washington profit corporation that has its principal place of business at 7700 NE Parkway Drive, Suite 300, Vancouver, Washington 98662.

JURISDICTION AND VENUE

30. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, including each Plaintiff, is a citizen of a state different from Defendant.

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

31. The Court has general personal jurisdiction over Defendant because, personally or through its agents, Defendant is registered a Washington corporation, it maintains its headquarters in Washington, and it committed the tortious acts complained of herein in Washington.

32. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because it is the district within which Prestige Care is headquartered and has the most significant contacts.

FACTUAL ALLEGATIONS

Defendant's Business

33. Defendant Prestige Care, founded in 1985, is "a complete senior care organization that includes independent living communities, assisted living, memory care, as well as skilled nursing and rehabilitation centers."[4]

34. Prestige Care has around or over 75 locations spread throughout eight states: Alaska, Arizona, Idaho, California, Montana, Nevada, Oregon, and Washington.[5]

35. For the purposes of this Consolidated Amended Class Action Complaint, all of Prestige Care's associated locations will be referred to collectively as "Prestige Care."

36. In the ordinary course of receiving assisted living care services from Defendant Prestige Care, or alternatively being employed by Prestige Care, each senior and employee must provide (and Plaintiffs did provide) Defendant Prestige Care with sensitive, personal, and private information, such as their:

- Name, address, phone number, and email address;
- Date of birth;
- Social Security number;

[4] https://www.prestigecare.com/about-prestige/ (last accessed Feb. 21, 2024).

[5] https://www.prestigecare.com/find-a-location/ (last accessed Feb. 21, 2024).

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

- Marital status;
- Contact information;
- Primary and secondary insurance policy holders' name, address, date of birth, and Social Security number;
- Demographic information;
- Driver's license or state or federal identification number;
- Medical history information;
- Insurance information and coverage; and
- Banking and/or credit card information.

37. Defendant also creates and stores medical records and other protected health information for its patients, records of treatments and diagnoses.

38. Plaintiffs and Class Member (electronically and in-person) transferred their Private Information to Defendant for the purposes of facilitating services from and employment with Defendant and with the agreement and understanding that the Private Information would be adequately safeguarded and/or destroyed within a reasonable time after the termination of the respective relationship.

39. By obtaining, collecting, receiving, and/or storing Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties to Plaintiffs and the Class, and it knew, or should have known, that it was thereafter responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

40. Defendant derived a substantial economic benefit from collecting Plaintiffs' and Class Members' Private Information. Without that Private Information, Defendant could not perform the services it provides.

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

41. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information, including but not limited to, protecting their usernames and passwords, using only strong passwords for their accounts, and refraining from browsing potentially unsafe websites.

42. On information and belief, Prestige Care's HIPAA Notice of Privacy Practices ("Privacy Policy") is provided to every senior, both prior to receiving services and upon request. Prestige Care's Privacy Notice makes clear that it understands that seniors Private Information is personal and must be protected by law.[6]

43. Defendant's Privacy Policy promises that "[a]t Prestige Care Inc., and Prestige Senior Living, L.L.C., we take your privacy seriously."[7]

44. Defendant's Privacy Policy promises to only disclose patient Private Information in limited circumstances, none of which includes a data breach.

45. On information and belief, all Plaintiffs transferred via one of Defendant's web properties at least some of the Private Information compromised in the Data Breach.

46. Defendant Prestige Care agreed to and undertook legal duties to maintain the protected health and personal information entrusted to it by Plaintiffs and Class Members safely, confidentially, and in compliance with all applicable laws, including the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, and the Health Insurance Portability and Accountability Act ("HIPAA").

47. Yet, through its failure to properly secure the Private Information of Plaintiffs and Class, Prestige Care failed to meet its own promises of patient privacy.

---

[6] https://www.prestigecare.com/privacy-policy/ (last accessed April 22, 2024).

[7] *Id.*

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

48. The information held by Defendant Prestige Care in its computer system and network included the highly sensitive Private Information of Plaintiffs and Class Members.

49. On information and belief, Defendant does not follow its own policies or industry standard practices in securing residents' and employee's PII.

50. On information and belief, Defendant failed to ensure the proper monitoring and logging of the ingress and egress of network traffic.

51. On information and belief, Defendant failed to ensure the proper monitoring and logging of file access and modifications.

52. On information and belief, Defendant failed to ensure the proper implementation of processes to quickly detect and respond to data breaches, security incidents, or intrusions.

53. On information and belief, Defendant failed to ensure the proper encryption of Plaintiff's and Class Members' Private Information and monitor user behavior and activity to identify possible threats.

54. On information and belief, Defendant inadequately trains its employees and cybersecurity partners on cybersecurity policies and then fails to enforce those policies.

55. On information and belief, Defendant failed to maintain reasonable and adequate security practices over its systems storing Plaintiff's and Class Members' PII.

The Data Breach

56. A data breach occurs when cyber criminals intend to access and steal Private Information that has not been adequately secured by a business entity like Prestige Care.

57. According to Defendant's website Notice, it learned of a cyber attack on its computer systems on or around September 7, 2023, when it took many of the healthcare provider's

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

networked systems offline, adversely affecting patient treatment, scheduling, and the ability to access patient histories.[8]

58. As of January 31, 2024, on information and belief, Prestige Care sent the required State Attorney Generals' notices of the Data Breach, and Plaintiffs and Class Members received direct notice that their Private Information was breached and exfiltrated.

59. On or about January 31, 2024, months after Prestige Care learned that Plaintiffs and Class Members Private Information was accessed and exfiltrated by cybercriminals, Plaintiffs and Class Members first began receiving their notices of the Data Breach.

60. Prestige Care's notice letters recommended time-consuming, generic steps that victims of data security incidents can take, such as getting a copy of a credit report or notifying law enforcement about suspicious financial account activity. Other than providing one year of credit monitoring that Plaintiffs and Class Members would have to affirmatively sign up for and a call center number that victims may contact with questions, Prestige Care offered no other substantive steps to help victims like Plaintiffs and Class Members to protect themselves. On information and belief, Prestige Care sent a similar generic letter to all individuals affected by the Data Breach.

61. Due to the actual and imminent risk of identity theft, Defendant instructs Plaintiffs and Class Members to do the following: "[w]e encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity."

62. Prestige Care's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

[8] https://www.prestigecare.com/notice-of-data-event/ (last accessed Feb. 21, 2024).

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

63. In January 2023, for example, the U.S. Department of Health & Human Services ("HHS") created a presentation specifically for healthcare providers and IT departments, warning entities like Prestige Care of the severe threats posed by Royal, BlackCat and similar cybercriminal groups.[9] Within the healthcare industry, the risk of a cyber attack is well-known and preventable with adequate security systems in place.

64. Prestige Care knew or should have known that its electronic records would be targeted by cybercriminals.

65. Prestige Care had obligations created by HIPAA, FTCA, contract, industry standards, common law, and representations made to Plaintiffs and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

66. Plaintiffs and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

The Data Breach was a
Foreseeable Risk of which Defendant was on Notice.

67. It is well known that PII, including Social Security numbers in particular, is a valuable commodity and a frequent, intentional target of cyber criminals. Companies that collect such information, including Prestige Care, are well-aware of the risk of being targeted by cybercriminals.

68. Individuals place a high value not only on their PII, but also on the privacy of that data. Identity theft causes severe negative consequences to its victims, as well as severe distress and hours of lost time trying to fight against the impact of identity theft.

[9] https://www.hhs.gov/sites/default/files/royal-blackcat-ransomware-tlpclear.pdf (last accessed Feb. 21, 2024).

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

69. A data breach increases the risk of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice, "[a] direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss." [10]

70. Individuals, like Plaintiffs and Class members, are particularly concerned with protecting the privacy of their Social Security numbers, which are the key to stealing any person's identity and, for a hacker's purpose, is likened to accessing your DNA.

71. Data Breach victims suffer long-term consequences when their Social Security numbers are taken and used by hackers. Even if they know their Social Security numbers are being misused, Plaintiffs and Class Members cannot obtain new numbers unless they become a victim of Social Security number misuse.

72. The Social Security Administration has warned that "a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So, using a new number

[10] "Victims of Identity Theft, 2018," U.S. Department of Justice (April 2021, NCJ 256085) available at https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last accessed Feb. 21, 2024).

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same."[11]

73. In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[12]

74. Additionally in 2021, there was a 15.1% increase in cyberattacks and data breaches over the prior year. Over the next two years, security executives predicted an increase in attacks from "social engineering and ransomware" as nation-states and cybercriminals grow more sophisticated. Unfortunately, these preventable causes will largely come from "misconfigurations, human error, poor maintenance, and unknown assets."[13]

75. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, are prepared for, and hopefully can ward off a cyberattack.

76. Despite the prevalence of public announcements of data breaches and data security compromises, despite its own acknowledgment of data security compromises, and despite its own acknowledgment of its duties to keep PII private and secure, Prestige Care failed to take appropriate steps to protect the PII of Plaintiffs and the proposed Class from being compromised.

Data Breaches are Rampant in Healthcare.

77. Defendant's data security obligations were particularly important given the substantial increase in data breaches in the healthcare industry preceding the date of the breach.

---

[11] https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Feb. 21, 2024).

[12] https://www.cnet.com/tech/services-and-software/record-number-of-data-breaches-reported-in-2021-new-report-says/ (last accessed Feb. 21, 2024).

[13] https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864 (last accessed Feb. 21, 2024).

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

78. According to an article in the HIPAA Journal posted on October 14, 2022, cybercriminals hack into medical practices for their "highly prized" medical records. "[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw 714 data breaches of 500 or more records reported to the [HHS' Office for Civil Rights] OCR – an 11% increase from the previous year. Almost three-quarters of those breaches were classified as hacking/IT incidents."[14]

79. Healthcare organizations are easy targets because "even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health insurance information, and medical and clinical data, and that information can be easily monetized."[15]

80. The HIPAA Journal article goes on to explain that patient records, like those stolen from Prestige Care, are "often processed and packaged with other illegally obtained data to create full record sets (fullz) that contain extensive information on individuals, often in intimate detail." The record sets are then sold on dark web sites to other criminals and "allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities."[16]

---

[14] https://www.hipaajournal.com/why-do-criminals-target-medical-records/ (last accessed Feb. 21, 2024).

[15] *Id.*

[16] *Id.*

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

81. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[17]

82. HHS data shows more than 39 million patients' information was exposed in the first half of 2023 in nearly 300 incidents, and healthcare beaches have doubled between 2020 and 2023, according to records compiled from HHS data by Health IT Security.[18]

83. According to Advent Health University, when an electronic health record "lands in the hands of nefarious persons the results can range from fraud to identity theft to extortion. In fact, these records provide such valuable information that hackers can sell a single stolen medical record for up to $1,000."[19]

84. The significant increase in attacks in the healthcare industry, and attendant risk of future attacks, is widely known to the public and to anyone in that industry, including Defendant Prestige Care.

Defendant Fails to Comply with FTC Guidelines.

85. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses that 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.

86. In October 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines

---

[17] *See* Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last accessed Feb. 21, 2024).

[18] https://healthitsecurity.com/features/biggest-healthcare-data-breaches-reported-this-year-so-far (last accessed Feb. 21, 2024).

[19] https://www.ahu.edu/blog/data-security-in-healthcare (last accessed Feb. 21, 2024).

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

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.[20] 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.[21]

87. 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.

88. The FTC has brought enforcement actions against businesses, like Prestige Care, 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 further clarify the measures businesses must take to meet their data security obligations.

89. These FTC enforcement actions include actions against healthcare providers 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 Commission concludes that

[20] *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 accessed Feb. 21, 2024).

[21] *Id.*

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

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

90. Defendant failed to properly implement basic data security practices.

91. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' and employees' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

92. Defendant was at all times fully aware of its obligation to protect the Private Information of its patients and employees. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards.

93. 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 that they collect and maintain.

94. Industry experts have also identified several best practices healthcare providers like Defendant should implement at a minimum, including but not limited to: educating all employees; utilizing strong passwords; creating multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; using multi-factor authentication; protecting backup data, and; limiting which employees can access sensitive data.

95. 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

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

96. 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.

97. These frameworks are existing and applicable industry standards in the healthcare industry, yet Defendant failed to comply with these accepted standards, thereby opening the door to, and failing to thwart, the Data Breach.

Defendant's Conduct Violates HIPAA.

98. HIPAA requires covered entities such as Defendant to protect against reasonably anticipated threats to the security of sensitive patient health information (PHI).

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

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

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

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).

101. A Data Breach such as the one Defendant experienced is considered a breach under the HIPAA rules because there is an access of PHI not permitted under the HIPAA Privacy Rule.

102. A breach under the HIPAA Rules is defined as ". . . the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.40.

103. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate it failed to comply with safeguards mandated by HIPAA regulations.

Defendant has Breached its Obligations to Plaintiffs and Class Members.

104. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and its patients' and employees' Private Information. Defendant's 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' and employees' Private Information;

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

d. Failing to ensure that vendors with access to Defendant's protected health data employed reasonable security procedures;

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

f. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

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

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

h. 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);

i. 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);

j. 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);

k. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce, in violation of 45 C.F.R. § 164.306(a)(4);

l. Failing to train all members of Defendant's workforce 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); and/or

m. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it 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 definition of encryption).

105. As a result of maintaining its computer systems in manner that required security upgrading, having inadequate procedures for handling emails containing ransomware or other malignant computer code, and inadequately training employees who opened files containing a ransomware virus, Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information.

106. Accordingly, as outlined below, Plaintiffs and Class Members now face an increased risk of fraud and identity theft.

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

Data Breaches Put Consumers at an Increased Risk Of Fraud and Identify Theft.

107. Data Breaches such as the one experienced by Plaintiffs and Class Members are especially problematic because of the disruption they cause to the overall daily lives of victims affected by the attack.

108. In 2019, the United States Government Accountability Office released a report addressing the steps consumers can take after a data breach. Its appendix of steps consumers should consider, in extremely simplified terms, continues for five pages. In addition to explaining specific options and how they can help, one column of the chart explains the limitations of the consumers' options. It is clear from the GAO's recommendations that the steps Data Breach victims (like Plaintiffs and Class) must take after a breach like Defendant's are both time consuming and of only limited and short-term effectiveness.

109. The GAO has long recognized that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record," discussing the same in a 2007 report as well ("2007 GAO Report").[22]

110. The FTC, like the GAO, 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 (and to consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting

[22] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last accessed July 19, 2023) ("2007 GAO Report").

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[23]

111. 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.

112. 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.

113. Theft of Private Information is also gravely serious. PII/PHI is a valuable property right.[24]

114. There may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered.

115. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

116. There is a strong probability that the entirety of the stolen information has been dumped on the black market or will be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

---

[23] *See* https://www.identitytheft.gov/Steps (last accessed Feb. 21, 2024).

[24] *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).

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

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

117. As the HHS warns, "PHI can be exceptionally valuable when stolen and sold on a black market, as it often is. PHI, once acquired by an unauthorized individual, can be exploited via extortion, fraud, identity theft and data laundering. At least one study has identified the value of a PHI record at $1000 each."[25]

118. Furthermore, 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 individual's authentic tax return is rejected.

119. 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

[25] https://www.hhs.gov/sites/default/files/cost-analysis-of-healthcare-sector-data-breaches.pdf at 2 (citations omitted) (last accessed Feb. 21, 2024).

[26] *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2018), available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Feb. 21, 2024).

[27] *Id.* at 4.

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

old number, so all of that old bad information is quickly inherited into the new Social Security number."[28]

120. 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]

121. In recent years, the medical and financial services industries have experienced disproportionally higher numbers of data theft events than other industries. Defendant therefore knew or should have known this and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

122. Fraudsters can also use medical information, including health insurance information, to commit healthcare fraud, including by submitting fraudulent requests for reimbursement to an individual's health insurance provider or obtaining healthcare in another individual's name. The individual typically does not discover the fraud until their health insurance premiums increase or they receive a bill for the service obtained in their name.

PLAINTIFFS' EXPERIENCES

Plaintiff Brim

---

[28] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last accessed Feb. 21, 2024).

[29] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Feb. 21, 2024).

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

123. Plaintiff Brim is a former Prestige Care employee who worked for Prestige from approximately 2012 through 2016.

124. To obtain employment from Defendant, Plaintiff Brim was required to provide her Private Information to Defendant, including her name, Social Security number, health insurance information, and medical information. Plaintiff Brim would not have entrusted her Private Information to Defendant had she known that Defendant would not take reasonable steps to safeguard her Private Information.

125. At the time the Data Breach was discovered on or around September 7, 2023, Prestige Care retained and maintained Plaintiff Brim's Private Information in its system—though she had not worked for them for approximately seven years.

126. Plaintiff Brim is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

127. Plaintiff Brim received the Notice Letter, by mail, directly from Defendant, dated January 31, 2024. According to the Notice Letter, Plaintiff Brim's Private Information was improperly accessed and obtained by unauthorized third parties, including her name, Social Security number, health insurance information, and medical information.

128. As a result of the Data Breach, and at the direction of Defendant's Notice Letter—which instructs all victims to "remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity"—Plaintiff Brim made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching and verifying the Data Breach and monitoring

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

her financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Brim has spent significant time dealing with the Data Breach, valuable time Plaintiff Brim otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

129. The Data Breach has caused Plaintiff Brim to suffer fear, anxiety, and stress, which has been compounded by the fact that Prestige Care has still not fully informed her of key details about the Data Breach.

130. As a result of the Data Breach and accompanying injuries, Plaintiff Brim anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Brim is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Perry

131. Plaintiff Perry is a former employee of Prestige Care. Plaintiff Perry received a Notice of Data Breach Letter dated January 31, 2024 informing her of Prestige Care's Data Breach.

132. The Notice Letter generically states that the files accessed in the Breach contain her "Social Security number, date of birth, employer assigned identification number, health insurance information, and [] name." The Notice Letter does not state what exact health insurance information was taken, and whether that included medical treatment information.

133. Plaintiff Perry is especially alarmed by the vagueness of the Notice Letter and equally by the fact that her Social Security number was identified as among the breached data on Prestige Care's computer system.

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

134. As a result of the Data Breach, and at the direction of Defendant's Notice Letter—which instructs victims to "remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity—Plaintiff Perry made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching and verifying the Data Breach and monitoring her financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Perry has spent significant time dealing with the Data Breach, valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

135. Since the Data Breach, Plaintiff Perry monitors her financial accounts for about an hour per week. This is more time than she spent prior to learning of the Prestige Care's Data Breach. Having to do this every week not only wastes her time as a result of Prestige Care's negligence, but it also causes her great anxiety.

136. Shortly after and as a result of the Data Breach, Plaintiff Perry began receiving an excessive number of spam calls on the same cell phone number she provided to Prestige Care for her employee records. These calls are a distraction, must be deleted, and waste time each day. On information and belief, the increase in spam phone calls is attributable to the Data Breach.

137. Plaintiff Perry receives many spam emails and texts now, which was not typical before the Data Breach. On information and belief, the increase in spam emails and texts is attributable to the Data Breach.

138. Plaintiff Perry is aware that cybercriminals often sell Private Information, and once stolen, it is likely to be abused months or even years after Prestige Care's Data Breach.

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

139. Had Plaintiff Perry been aware that Prestige Care's computer systems were not secure, she would not have entrusted Prestige Care with her PII and PHI.

140. As a result of the Data Breach and accompanying injuries, Plaintiff Perry anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Perry is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Turner Lamonica

141. Plaintiff Turner Lamonica is a former employee of Prestige Care.

142. As a condition of her employment with Defendant, Plaintiff Turner Lamonica entrusted her Private Information to Defendant with the reasonable expectation and understanding that Defendant would take, at a minimum, industry standard precaution to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to her. Plaintiff Turner Lamonica would not have entrusted her Private Information to Defendant had she known that Defendant would not take reasonable steps to safeguard her Private Information.

143. In January 2024, months after Defendant learned of the Data Breach, Plaintiff Turner Lamonica received a letter from Defendant, notifying her that her Private Information had been improperly accessed and/or obtained by unauthorized third parties in the Data Breach.

144. As a result of the Data Breach and at Defendant's recommendations, Plaintiff Turner Lamonica made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to researching the Data Breach and reviewing credit card and financial account statements. She also intends to order a

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

copy of her credit report and reach out to her insurance company to review those records to ensure that he has not been subject to any fraud. She also has and is in the process of changing passwords. She is also researching credit monitoring services to find an affordable option.

145. Plaintiff Turner Lamonica has spent multiple hours attempting to mitigate the effects of the Data Breach and safeguard herself from its consequences. She will continue to spend time she otherwise would have spent on other activities, including, but not limited to, work and/or recreation.

146. Plaintiff Turner Lamonica has also suffered emotional distress as a result of the release of her Private Information—which she believed would be protected from unauthorized access and disclosure—including anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of identity theft and fraud. Plaintiff Turner Lamonica is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach. Plaintiff Turner Lamonica also has suffered anxiety about unauthorized parties viewing, using, and/or publishing information related to her medical records and prescriptions.

147. As a result of the Data Breach and its accompanying injuries, Plaintiff Turner Lamonica anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Turner Lamonica will continue to be at a present, imminent, and continued increased risk of identity theft and fraud in perpetuity.

PLAINTIFFS' AND CLASS MEMBERS' INJURIES

148. To date, Defendant Prestige Care has done absolutely nothing to compensate Plaintiffs and Class Members for the damages they sustained in the Data Breach.

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

149. Defendant Prestige Care has merely offered one year of credit monitoring services through Cyberscout, a tacit admission that its failure to protect their Private Information has caused Plaintiffs and Class great injuries that will continue into the future. These limited services are inadequate when victims are likely to face many years of identity theft.

150. Prestige Care's offer fails to sufficiently compensate victims of the Data Breach, who commonly face multiple years of ongoing identity theft, and it entirely fails to provide any compensation for its unauthorized release and disclosure of Plaintiffs' and Class Members' Private Information, out of pocket costs, and the time they are required to spend attempting to mitigate their injuries.

151. Furthermore, Defendant Prestige Care's credit monitoring offer and advice to Plaintiffs and Class Members squarely places the burden on Plaintiffs and Class Members, rather than on the Defendant, to investigate and protect themselves from Defendant's tortious acts resulting in the Data Breach. Defendant merely sent instructions to Plaintiffs and Class Members about actions they can affirmatively take to protect themselves.

152. Plaintiffs and Class Members have been damaged by the compromise and exfiltration of their Private Information in the Data Breach and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

153. Plaintiffs' and Class Members' Private Information was compromised and exfiltrated by cyber-criminals as a direct and proximate result of the Data Breach.

154. Plaintiffs and Class were damaged in that their Private Information is now in the hands of cyber criminals, sold and potentially for sale for years into the future.

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

155. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been placed at an actual, imminent, and substantial risk of harm from fraud and identity theft.

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

157. Plaintiffs 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. Plaintiffs 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.

158. Plaintiffs 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 Plaintiffs and Class Members.

159. Plaintiffs 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.

160. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time monitoring their financial accounts and records for misuse.

161. Plaintiffs 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-

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

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 services;

d. Monitoring their medical records for fraudulent charges and data;

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

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

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

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

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

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

k. 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

l. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

162. Plaintiffs and Class Members have an interest in ensuring that their Private 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 personal and financial information as well as health information is not accessible online and that access to such data is password-protected.

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

163. As a result of Defendant's conduct, Plaintiffs 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—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

164. Defendant's delay in identifying and reporting the Data Breach caused additional harm. In a data breach, time is of the essence to reduce the imminent misuse of PII and PHI. Early notification helps a victim of a Data Breach mitigate their injuries, and in the converse, delayed notification causes more harm and increases the risk of identity theft. Here, Prestige Care knew of the breach since September 7, 2023 and did not notify the victims until January 31, 2024. Yet Prestige Care offered no explanation of purpose for the delay. This delay violates HIPAA and other notification requirements, and it increases the injuries to Plaintiffs and Class.

CLASS ACTION ALLEGATIONS

165. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated.

166. Plaintiffs propose the following Class definition, subject to amendment as appropriate:

> All individuals residing in the United States whose Private Information was compromised as a result of the Data Breach discovered by Prestige Care, Inc., in September 2023 and to whom it provided notice in 2024 (the "Class").

167. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant; and members of the judiciary to whom this case is assigned, their families and Members of their staff.

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

168. Plaintiffs hereby reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery. The proposed Class meets the criteria for certification Fed. R. Civ. P. Rule 23.

169. Numerosity, Fed. R. Civ. P. 23(a)(1): The Members of the Class are so numerous that joinder of all of them is impracticable. The number class members is believed to be around 38,087 people.

170. Commonality. As required by Fed. R. Civ. P. 23(a)(2) and (b)(3), there are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

b. 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;

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

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

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

g. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

j. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and

k. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

171. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class member, was compromised in the Data Breach.

172. Adequacy of Representation, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

173. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

174. Superiority, Fed. R. Civ. P. 23(b)(3): A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

175. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis. Further, Plaintiff and Class Members have an interest in ensuring that their Personal 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 personal and financial information is not accessible online, is encrypted, and is password-protected. Damages from a future breach due to Defendant's inadequate data security represent an irreparable injury (such as the further loss of privacy and exposure of PII such as social security numbers) for which no adequate remedy at law exists.

176. Likewise, particular issues are appropriate for certification under Rule 23(c)(4) 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 failed to timely notify the public of the Data Breach;

b. whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. whether Defendant's failure to institute adequate protective security measures amounted to negligence;

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

e. whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

f. whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach; and

g. whether Defendant failed to abide by its responsibilities under HIPAA.

177. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CLAIMS FOR RELIEF

First Count
Negligence
(On Behalf of Plaintiffs and Class Members)

178. Plaintiffs reallege and incorporate the above allegations as if fully set forth herein.

179. Defendant Prestige Care required Plaintiffs and Class Members to submit non-public Private Information to Prestige to obtain assisted living services and/or employment.

180. By collecting and storing this data in Prestige Care's computer systems, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer systems—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a Data Breach.

181. Defendant owed a duty of care to Plaintiffs 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.

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

183. Defendant's duty to use reasonable security measures under HIPAA required Defendant 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). Some or all of the healthcare, medical, and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

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

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

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

186. Defendant breached its duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant 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 their networks and systems;

c. failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. allowing unauthorized access to Class Members' Private Information;

e. failing to detect in a timely manner that Class Members' Private Information had been compromised; and

f. failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

187. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injuries to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

188. 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.

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

189. Defendant's negligence was the proximate cause and cause-in-fact of Plaintiffs' and Class Members' injuries and damages stemming from the Data Breach.

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

191. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiffs and Class Members in an unsafe and unsecure manner.

192. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant 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 monitoring to all Class Members.

Second Count
Breach of Implied Contract
(On Behalf of Plaintiffs and Class Members)

193. Plaintiffs reallege and incorporate the above allegations as if fully set forth herein.

194. When Plaintiffs and Class Members provided their Private Information to Defendant Prestige Care in exchange for Defendant's assisted living services or employment, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

195. Defendant solicited, offered, and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

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

197. Plaintiffs and Class Members provided valuable Private Information, paid monies, and provided employment services to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings therefrom to obtain adequate data security. Defendant failed to do so.

198. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

199. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

200. Through Defendant's acceptance of Private Information, employment services, and monies for medical goods and services, it knew or should have known that it must protect Plaintiffs' and Class Members' confidential Personal Information in accordance with its policies, practices, industry standards, and applicable law.

201. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

202. Defendant breached its implied contracts with Plaintiffs and Class Members by failing to safeguard and protect Plaintiffs' and Class Members' Private Information.

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

203. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiffs and Class Members sustained damages as alleged herein, including the loss of the benefit of the bargain.

204. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

205. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate long-term credit monitoring to all Class Members.

Third Count
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and Class Members)

206. Plaintiffs reallege and incorporate the above allegations as if fully set forth herein.

207. In light of the special relationship between Defendant Prestige Care and Plaintiffs and Class Members, whereby Defendant became guardian of Plaintiffs' and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiffs and Class Members, (1) for the safeguarding of Plaintiffs' and Class Members' Private Information; (2) to timely notify Plaintiffs 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.

208. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its relationship with its current and former patients and employees to keep secure their Private Information.

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

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

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

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

212. Defendant breached its fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

213. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs 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

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

Breach for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of Defendant's services they received.

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

Fourth Count
Unjust Enrichment
(On Behalf of Plaintiffs and Class Members)

215. Plaintiffs reallege and incorporate the above allegations as if fully set forth herein.

216. This Count is pleaded in the alternative to Plaintiffs' claim for Breach of Implied Contract.

217. On information and belief, Defendant funds its data security measures entirely from its general revenue, including funds made as a result of the labor or amounts received from Plaintiffs and the Class Members.

218. A portion of the revenue made as a result of the labor or amounts received from Plaintiffs and the Class Members should have been used to provide a reasonable level of data security.

219. Plaintiffs and Class Members conferred a monetary benefit on Defendant. In exchange, Plaintiff and Class Members should have received adequate data security protecting their Private Information.

220. Defendant knew that Plaintiffs and Class Members conferred a benefit that Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

221. Defendant unjustly enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead chose to avoid its data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

222. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money that should have been used on data security because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

223. Defendant acquired this monetary benefit and Personal Information through inequitable means in that it failed to disclose its inadequate security practices.

224. If Plaintiffs and Class Members knew that Defendant had not secured their Personal Information, they would not have agreed to provide their Personal Information to Defendant.

225. Plaintiffs and Class Members have no adequate remedy at law.

226. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to dictate how their Private Information is used; (iii) the compromise, publication, and/or theft of their Personal Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Personal Information; (v) lost opportunity costs associated with effort expended and

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

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; (vi) the continued risk to their Personal 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 Personal Information in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Personal Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

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

228. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that it unjustly received from them.

Fifth Count
Declaratory Judgment
(On Behalf of Plaintiffs and Class Members)

229. Plaintiffs reallege and incorporate the paragraphs above as if fully set forth herein.

230. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

231. An actual controversy has arisen in the wake of the Defendant's Data Breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' Personal Information and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class members from further data breaches that compromise their Private Information.

232. Plaintiffs allege that Defendant's data security measures remain inadequate. Plaintiffs will continue to suffer injury because of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future.

233. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant continues to owe a legal duty to secure patients' Private Information and to timely notify patients of a data breach under the common law, HIPAA, Section 5 of the FTC Act, and various states' statutes; and

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure patients' Private Information.

234. The Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect patients' Private Information.

235. If an injunction is not issued, Plaintiffs and Class members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, Plaintiffs and Class members will not have an adequate remedy at law because many of

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

236. The hardship to Plaintiffs and Class members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another massive data breach occurs at Defendant, Plaintiffs and Class members will likely be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has pre-existing legal obligations to employ such measures.

237. Issuance of the requested injunction will not do a disservice to the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiffs and the millions of individuals whose Private Information would be further compromised.

Sixth Count
Violations of the Washington State Consumer Protection Act, RCW 19.86.010, *et seq*.
(On Behalf of Plaintiffs and Class Members)

238. Plaintiffs reallege and incorporate the paragraphs above as if fully set forth herein.

239. The Washington Consumer Protection Act, RCW 19.86.020 (the "CPA") prohibits any "unfair or deceptive acts or practices" in the conduct of any trade or commerce as those terms are described by the CPA and relevant case law.

240. Defendant is a "person" as described in RCW 19.86.010(1).

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

241. Defendant engages in "trade" and "commerce" as described in RCW 19.86.010(2) in that it engages in the sale of services and commerce directly and indirectly affecting the people of the State of Washington.

242. Defendant is headquartered in Washington; its strategies, decision-making, and commercial transactions originate in Washington; most if not all of its key operations and employees reside, work, and make company decisions (including data security decisions) in Washington; and Defendant and many of its employees are part of the people, residents, and citizens of the State of Washington.

243. In the course of conducting its business, Defendant committed "unfair acts or practices" by, among other things, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiffs' and Class Members' Private Information. Plaintiffs and Class Members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. As described above, Defendant's unfair acts and practices are ongoing and continue to this date.

244. Defendant's conduct was also deceptive. Defendant failed to timely notify and concealed from Plaintiffs and Class Members the unauthorized release and disclosure of their Private Information. If Plaintiffs and Class Members had been notified in an appropriate fashion, and had the information not been hidden from them, they could have taken earlier and more robust precautions to safeguard and protect their Private Information and identities.

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

245. Defendant's "unfair or deceptive acts or practices" affect the public interest because they are substantially injurious to persons, they had the capacity to injure other persons, and they have the capacity to injure other persons.

246. The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in its wrongful conduct.

247. Defendant's unfair and deceptive acts and practices directly and proximately caused injury to Plaintiffs and Class Members' businesses and property. Plaintiffs and Class Members have suffered, and will continue to suffer, actual damages and injury in the form of, among other things, (1) an imminent, immediate and the continuing increased risk of identity theft, identity fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (2) invasion of privacy; (3) breach of the confidentiality of their Private Information; (4) deprivation of the value of their Private Information, for which there is a well-established national and international market; (5) the financial and temporal cost of monitoring credit, monitoring financial accounts, and mitigating damages; and/or (6) investment of substantial time and money to monitoring and remediating the harm inflicted upon them.

248. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiffs, therefore, on behalf of themselves, Class Members, and the general public, also seek restitution and an injunction prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to modify its corporate culture and design, adopt, implement, control, direct, oversee, manage,

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect Private Information.

249. Plaintiffs, on behalf of themselves and the Class, also seek to recover actual damages sustained by each Class Member together with the costs of the suit, including reasonable attorneys' fees. In addition, Plaintiffs, on behalf of themselves and the Class, request that this Court use its discretion under RCW 19.86.090 to increase the damages award for each class member to three times the actual damages sustained, not to exceed $25,000.00 per class member.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

a) For an Order certifying this action as a class action and appointing Plaintiffs and their 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 Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

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

e) Ordering Defendant to pay for not less than ten years of credit monitoring services for Plaintiffs and the Class;

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

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

h) For pre- and post-judgment interest on any amounts awarded; and

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

i) For such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all claims so triable.

Dated: April 30, 2024

Respectfully submitted,

By: /s/ *Gary E. Mason*

Gary E. Mason, admitted *pro hac vice*
Danielle L. Perry, admitted *pro hac vice*
Lisa A. White, admitted *pro hac vice*
MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015
Tel: (202) 429-2290
gmason@masonllp.com
dperry@masonllp.com
lwhite@masonllp.com

/s/ Kaleigh N. Boyd
Kaleigh N. Boyd, WSBA No. 52684
TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth A venue, Suite 1700
Seattle, WA 98101
Tel: (206) 682-5600
Fax: (206) 682-2992
kboyd@tousley.com

Local Counsel

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel: (202) 429-2290
gklinger@milberg.com

Bryan L. Bleichner*
Philip J. Krzeski, admitted *pro hac vice*
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Tel: (612) 339-7300
Fax: (612) 336-2940

bbleichner@chestnutcambronne.com
pkrzeski@chestnutcambronne.com

*pro hac vice to be submitted

Interim Class Counsel

MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290