CAUSE NO. DC-24-09642

NORMA COVEY, LEWIS BENAVIDES, ROBERT LEIGH-MANUELL, DAVID HICKEY, and MARK BENNETT on behalf of themselves and all others similarly situated,	IN THE DISTRICT COURT
Plaintiffs, v.	DALLAS COUNTY, TEXAS
TEXAS RETINA ASSOCIATES,	
Defendant.	101st JUDICIAL DISTRICT

PLAINTIFFS' CONSOLIDATED CLASS ACTION PETITION

Plaintiffs Norma Covey, Lewis Benavides, Robert Leigh-Manuell, David Hickey, and Mark Bennett (collectively "Plaintiffs") bring this Class Action Petition ("Petition") against Texas Retina Associates ("TRA" or "Defendant") individually and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigation, and upon information and belief as to all other matters, as follows:

SUMMARY OF ACTION

1. Plaintiffs bring this class action against Defendant for its failure to properly secure and safeguard the sensitive personal information of its patients.

2. Defendant "is Texas' largest, most experienced ophthalmology practice" with 15 offices throughout the state.[1]

3. On March 27, 2024, an unauthorized third party gained access to the Defendant's network and computer systems and obtained unauthorized access to and exfiltrated Defendant's files containing Plaintiffs' and Class Members' sensitive personal information (the "Data

[1] https://www.texasretina.com/about-us

Breach").[2]

4. Plaintiffs' and Class Members' sensitive personal information—which they entrusted to Defendant on the mutual understanding that Defendant would protect it against disclosure—was targeted, compromised, and unlawfully accessed due to the Data Breach.

5. Defendant collected and maintained certain personally identifiable information and protected health information of Plaintiffs and the putative Class Members (defined below), who are (or were) patients at Defendant.

6. The personal information compromised in the Data Breach included Plaintiffs' and Class Members' full names, Social Security numbers, addresses, dates of birth ("personally identifiable information" or "PII") and medical and health insurance information, which is protected health information ("PHI", and collectively with PII, "Private Information")[3] as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

7. The Private Information compromised in the Data Breach was exfiltrated by cyber-criminals and remains in the hands of those cyber-criminals who target Private Information for its value to identity thieves.

8. As a result of the Data Breach, Plaintiffs and Class Members suffered concrete injuries in fact including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of their Private Information consisting

[2] https://oag.my.site.com/datasecuritybreachreport/apex/datasecurityreportspage and https://hackmanac.com/news/hacks-of-today-23-04-2024

[3] https://oag.my.site.com/datasecuritybreachreport/apex/datasecurityreportspage

of an increase in spam calls, texts, and/or emails; (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.

9. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect its patients' Private Information from a foreseeable and preventable cyber-attack.

10. Moreover, upon information and belief, Defendant was targeted for a cyber-attack due to its status as a healthcare entity that collects and maintains highly valuable Private Information on its systems.

11. Defendant maintained, used, and shared the Private Information in a reckless manner. In particular, the Private Information was used and transmitted by Defendant in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack 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.

12. 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 take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

13. Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct because the Private Information that Defendant collected and maintained has been accessed and acquired by data thieves.

14. Armed with the Private Information accessed in the Data Breach, data thieves have already engaged in identity theft and fraud and can in the future commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

15. As a result of the Data Breach, 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 in the future closely monitor their financial accounts to guard against identity theft.

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

17. Plaintiffs bring this class action lawsuit on behalf all those 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 the unauthorized access by an unknown third party and precisely what specific type of information was accessed.

18. Through this Petition, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data

Breach.

19. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction over this controversy because the contract between Plaintiffs and Defendant was established in Texas. Moreover, the Defendant's failure to adequately safeguard Class Members' data, i.e., the site of Defendant's negligent conduct, occurred in Dallas County, Texas. Plaintiffs have been damaged in a sum within the jurisdictional limits of this Court. Pursuant to Texas Rule of Civil Procedure 47, Plaintiffs seek monetary relief over $1,000,000.00.

21. This Court has personal jurisdiction over Defendant because it is a resident and citizen of Dallas County, Texas.

22. Venue is proper in this county under Tex. Civ. Prac. & Rem. Code § 15.002 because a substantial part of the events or omissions giving rise to the claim occurred in Dallas County, Texas.

23. Upon information and belief, at least two-thirds of the Class are citizens of Texas.

24. Upon information and belief, Plaintiffs' individual damages are less than $75,000.

PARTIES

25. Plaintiff Norma Covey is a resident and citizen of the State of Texas.

26. Plaintiff Lewis Benavides is a resident and citizen of the State of Texas.

27. Plaintiff Robert Leigh-Manuell is a resident and citizen of the State of Texas.

28. Plaintiff David Hickey is a resident and citizen of the State of Texas.

29. Plaintiff Mark Bennett is a resident and citizen of the State of Texas.

30. Defendant Texas Retina Associates is a professional association with its principal

place of business located at 9600 N. Central Expressway, Suite 100, Dallas, Texas 75231. The registered agent for service of process is Jefferey T. Brockette, 9600 N. Central Expressway, Suite 100, Dallas, Texas 75231. Defendant is a citizen of Texas.

DISCOVERY CONTROL PLAN

31. Due to the complexity of this case, discovery should be conducted pursuant to a discover control plan under Level 3, pursuant to Texas Rule of Civil Procedure 190.4. Plaintiffs affirmatively plead that this suit is not governed by the expedited actions process of Texas Rules of Civil Procedure 169 because Plaintiffs seek monetary relief in excess of $250,000.00.

FACTUAL ALLEGATIONS

Defendant's Business

32. Defendant is a Texas-based healthcare provider that operates "15 offices throughout the state with 17 retina-fellowship-trained physicians."[4]

33. Plaintiffs and Class Members are current and former patients of Defendant.

34. In the course of their relationship, patients, including Plaintiffs and Class Members, provided Defendant with at least the following: names, dates of birth, addresses, Social Security numbers, medical and health insurance information, and other sensitive information.

35. Upon information and belief, in the course of collecting Private Information from patients, including Plaintiffs, Defendant promised to provide confidentiality and adequate security for the data it collected from patients through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

36. Indeed, Defendant provides on its website that: "[w]e will take appropriate steps to protect your privacy and take reasonable security measures to protect your personal information

[4] https://www.texasretina.com/about-us

in storage."[5]

37. Defendant further states:

> We understand the importance of privacy and are committed to maintaining the confidentiality of your medical information. We make a record of the medical care we provide and may receive such records from others. We use these records to provide or enable other health care providers to provide quality medical care, to obtain payment for services provided to you as allowed by your health plan and to enable us to meet our professional and legal obligations to operate this medical practice properly. We are required by law to maintain the privacy of protected health information, to provide individuals with notice of our legal duties and privacy practices with respect to protected health information, and to notify affected individuals following a breach of unsecured protected health information. [6]

38. Defendant additionally has a HIPAA policy on its website, which states:

> Except as described in this Notice of Privacy Practices, this medical practice will, consistent with its legal obligations, not use or disclose health information which identifies you without your written authorization. If you do authorize this medical practice to use or disclose your health information for another purpose, you may revoke your authorization in writing at any time [7]

39. Plaintiffs and the Class Members, as patients of Defendant, relied on these promises and on this sophisticated business entity to keep their sensitive Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Patients, in general, demand security to safeguard their Private Information, especially when their PHI and other sensitive Private Information is involved.

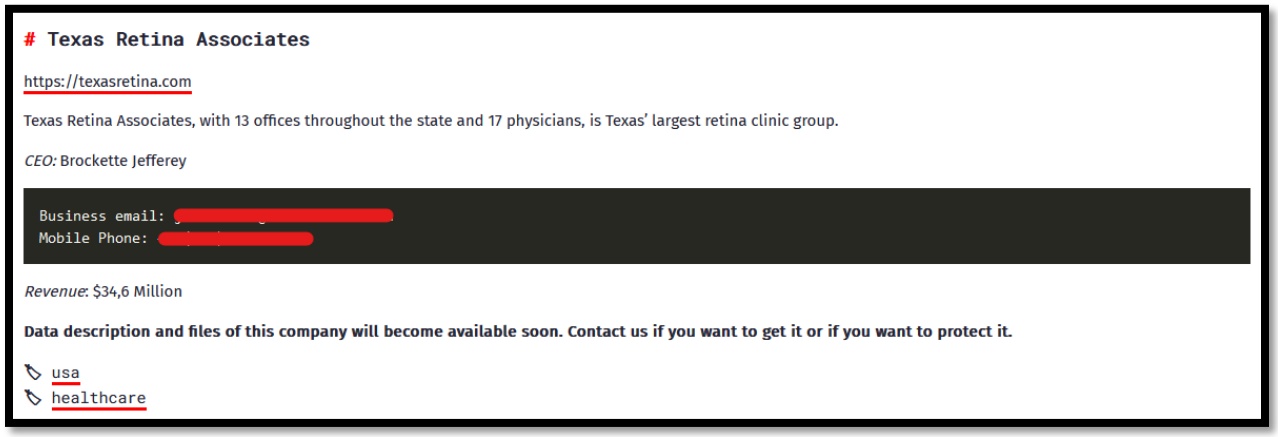
The Data Breach

40. On or about March 27, 2024, Defendant discovered that an infamous criminal hacking group called "BianLian" managed to access the network on which it stored the unencrypted Private Information Plaintiffs and Class Members and exfiltrated the Private

[5] https://www.texasretina.com/privacy-policy
[6] https://www.texasretina.com/wp-content/uploads/2018/06/informationpractices.pdf
[7] *Id.*

Information stored thereon. [8]

41. Shortly thereafter, BianLian took credit for the cyberattack and began offering the Private Information exfiltrated from Defendant's network on dark web forums: [9]



42. First appearing in late 2021, BianLian has claimed credit for at least 46 confirmed ransomware attacks.[10] The BianLian ransomware group is "known for its sophisticated attacks primarily in North America and Europe."[11]

43. The State of Texas requires that any "person who conducts business in this state and owns or licenses computerized data that includes sensitive personal information shall disclose any breach of system security, after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Tex. Bus. & Com. Code Ann. § 521.053(b). In fact, "breach of a security system" is defined as "[the] unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information." Tex.

[8] https://www.breachsense.com/breaches/texas-retina-data-breach/; https://www.linkedin.com/posts/redpacket-security_bianlian-ransomware-victim-texas-retina-activity-7188432333811646464-vA3V/; https://x.com/Comparitech/status/1782430118222143803?mx=2.
[9] https://hackmanac.com/news/hacks-of-today-23-04-2024
[10] https://www.comparitech.com/news/texas-retina-associates-notifies-300k-texans-of-data-breach-that-compromised-ssns-medical-info/
[11] *Id.*

Bus. & Com. Code Ann. § 521.053(a).

44. Because Defendant eventually issued the data breach notification disclosure as required by Tex. Bus. & Com. Code. Ann. § 521.053, following the investigation, Defendant must have concluded that Plaintiffs' and Class Members' **"sensitive personal information was, or is reasonably believed to have been acquired by an unauthorized person."** Tex. Bus. & Com. Code Ann. § 521.053.

45. However, despite knowing that Plaintiffs' and the Class's Private Information were in the hands of a notorious cyberhacker, Defendant delayed notification until at least June 26, 2024, when Defendant notified the Attorney General of Texas of the Data Breach. On or about June 28, 2024, Defendant posted a "Notice of Data Breach" on its website, informing victims, in relevant part, that:

> Texas Retina is committed to protecting the privacy and security of the personal information we maintain. We are making individuals aware of an incident that may affect the privacy of certain individuals' information. We are providing notice of the incident so that potentially affected individuals may take steps to protect their information, should they feel it appropriate to do so.
>
> **What Happened?** On March 27, 2024, Texas Retina detected unusual activity on our network. After identifying this, Texas Retina took steps to evaluate and ensure the security of our systems and networks. Further, we immediately engaged third-party independent cybersecurity experts to conduct an investigation into the incident.
>
> Our investigation determined that an unauthorized actor accessed our systems beginning on October 8, 2023, and, as a result, may have accessed or obtained certain files. We have been in the process of conducting an exhaustive review to identify the potentially impacted individuals whose personal information or protected health information was included within the files that may have been accessed or obtained from our network by an unauthorized actor as a result of the incident. To date, we have no evidence of financial fraud or identity theft arising out of the incident. Out of an abundance of caution, we are providing notice of the incident to individuals whose information was potentially impacted and explaining the services we are making available.

What Information was Involved? The personal information contained within the impacted data included first and last name, address, phone number, email address, date of birth, gender, Social Security number, medical record number, clinical information, prescription information, medical information, health information, and/or health insurance information. The types of impacted information varied by individual.

What We Are Doing. The security and privacy of the information contained within our systems is a top priority for us. In response to this incident, we took immediate steps to secure our systems and engaged third-party forensic experts to assist in the investigation. Further, we are implementing additional cybersecurity safeguards, as needed, enhancing our employee cybersecurity training, and improving our cybersecurity policies, procedures, and protocols to help minimize the likelihood of this type of incident occurring again.

How Will Individuals Know If They Are Affected By This Incident? Texas Retina is providing notice to individuals whose information was determined to be in the affected files in accordance with our legal obligations, to the best of our ability and to the extent we have valid mailing addresses. If an individual does not receive a letter but would like to know if they are affected, they may call 888-498-3901.

What You Can Do. We encourage individuals to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, explanation of benefits forms, and monitoring your free credit reports for suspicious activity and to detect errors. Under U.S. law individuals are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of their credit report, place a fraud alert, or a security freeze.[12]

46. Defendant has failed to provide information regarding the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. Plaintiff Benavides' Breach Notice is attached as Exhibit A. To date, these omitted details have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

47. As a result, Plaintiffs' and Class Members' ability to mitigate the harms resulting

[12] Breach Notice

from the Data Breach is severely diminished.

48. Through its Breach Notice, Defendant recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to "remain vigilant in reviewing your financial account statements, explanation of benefits statements, and credit reports for fraudulent or irregular activity on a regular basis." Ex. A

49. Also through the Data Breach Notice, Defendant recognized its duty to implement reasonable cybersecurity safeguards or policies to protect patients' Private Information, insisting that, despite the Data Breach demonstrating otherwise, it is "committed to maintaining the privacy of personal information in our possession" and "the privacy and security of the personal information we maintain is of the utmost importance to Texas Retina Associates." Ex. A.

50. On information and belief, Defendant has offered several months of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves Private Information that cannot be changed, such as Social Security numbers.

51. Defendant had obligations created by the FTC Act, HIPAA, contract, common law, and industry standards to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

52. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiffs and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

53. The attacker targeted, accessed, and acquired files containing unencrypted Private Information of Plaintiffs and Class Members. Plaintiffs' and Class Members' Private Information

was accessed and stolen in the Data Breach.

54. Plaintiffs further believe that their Private Information and that of Class Members was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type, and specifically, Bian Lian ransomware gang.

Data Breaches Are Preventable

55. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiffs and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

56. Defendant could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing Private Information.

57. A ransomware attack is a type of cyberattack that is frequently used to target healthcare providers due to the sensitive patient data they maintain.[13] In a ransomware attack the attackers use software to encrypt data on a compromised network, rendering it unusable and demanding payment to restore control over the network.[14] Ransomware attacks are particularly harmful for patients and healthcare providers alike as they cause operational disruptions that result in lengthier patient stays, delayed procedures or test results, increased complications from surgery, and even increased mortality rates.[15] In 2021, 44% of healthcare providers who experienced a ransomware attack saw their operations disrupted for up to a week and 25% experienced disrupted

[13] https://www.zdnet.com/article/ransomware-warning-now-attacks-are-stealing-data-as-well-as-encrypting-it/
[14] https://www.cisa.gov/stopransomware/ransomware-faqs
[15] https://www.healthcareitnews.com/news/ponemon-study-finds-link-between-ransomware-increased-mortality-rate

services for up to a month.[16]

58. Companies should treat ransomware attacks as any other data breach incident because ransomware attacks don't just hold networks hostage, "ransomware groups sell stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[17] As cybersecurity expert Emisoft warns, "[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence […] the initial assumption should be that data may have been exfiltrated."

59. An increasingly prevalent form of ransomware attack is the "encryption+exfiltration" attack in which the attacker encrypts a network and exfiltrates the data contained within.[18] In 2020, over 50% of ransomware attackers exfiltrated data from a network before encrypting it.[19] Once the data is exfiltrated from a network, its confidential nature is destroyed and it should be "assume[d] it will be traded to other threat actors, sold, or held for a second/future extortion attempt."[20] And even where companies pay for the return of data attackers often leak or sell the data regardless because there is no way to verify copies of the data are destroyed.[21]

60. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[22]

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

- Implement an awareness and training program. Because end users are targets,

[16]https://assets.sophos.com/X24WTUEQ/at/4wxp262kpf84t3bxf32wrctm/sophos-state-of-ransomware-healthcare-2022-wp.pdf
[17] https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends
[18]://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/
[19] https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report
[20] *Id*.
[21] *Id*.
[22] https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

employees and individuals should be aware of the threat of ransomware and how it is delivered.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[23]

[23] *Id.* at 3-4.

62. To prevent and detect cyber-attacks or ransomware attacks, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure Internet-Facing Assets

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

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

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

Build credential hygiene

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

Apply principle of least-privilege

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

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications].[24]

63. Given that Defendant was storing the Private Information of its current and former patients, Defendant could and should have implemented all of the above measures to prevent and

[24] https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/

detect cyberattacks.

64. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and data thieves acquiring and accessing the Private Information of, upon information and belief, thousands to tens of thousands of individuals, including that of Plaintiffs and Class Members.

Defendant Acquires, Collects, And Stores Patients' Private Information

65. Defendant acquires, collects, and stores a massive amount of Private Information on its current and former patients.

66. As a condition of obtaining services at Defendant, Defendant requires that patients entrust it with highly sensitive personal information.

67. Defendant retains and stores this information and derives a substantial economic benefit from the Private Information that they collect. But for the collection of Plaintiffs' and Class Members' Private Information, Defendant would be unable to perform its services.

68. By obtaining, collecting, and using Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from disclosure.

69. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and would not have entrusted it to Defendant absent a promise to safeguard that information.

70. Upon information and belief, in the course of collecting Private Information from patients, including Plaintiffs, Defendant promised to provide confidentiality and adequate security for their data through its applicable privacy policy and through other disclosures in compliance

with statutory privacy requirements.

71. Indeed, Defendant provides numerous assurances on its website, including that "[w]e will take appropriate steps to protect your privacy and take reasonable security measures to protect your personal information in storage."[25]

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

Defendant Knew, Or Should Have Known, of the Risk Because Healthcare Entities In Possession Of Private Information Are Particularly Susceptible To Cyber Attacks

73. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members and the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs and loss of time that would be imposed on Plaintiffs and Class Members as a result of a breach.

74. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on its network, amounting to thousands of individuals' detailed, Private Information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

75. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting healthcare entities that collect and store Private Information, like Defendant, preceding the date of the breach.

76. Data breaches, including those perpetrated against healthcare entities that store Private Information in their systems, have become widespread.

[25] https://www.texasretina.com/privacy-policy

77. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.[26]

78. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including HCA Healthcare (11 million patients, July 2023), Managed Care of North America (8 million patients, March 2023), PharMerica Corporation (5 million patients, March 2023), HealthEC LLC (4 million patients, July 2023), ESO Solutions, Inc. (2.7 million patients, September 2023), Prospect Medical Holdings, Inc. (1.3 million patients, July-August 2023), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

79. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store Private Information are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[27]

80. Additionally, as companies became more dependent on computer systems to run their business,[28] *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[29]

---

[26] https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/

[27] https://www.law360.com/patientprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=patientprotection

[28] https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html

[29] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022

81. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[30]

82. Defendant knew and understood unprotected or exposed Private Information in the custody of insurance companies, like Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that Private Information through unauthorized access.

83. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

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

85. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

86. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiffs and Class Members are long lasting and severe. Once Private Information is stolen—particularly PHI—fraudulent use of that information and damage to victims may continue for years.

87. As a healthcare entity in custody of the Private Information of its patients, Defendant knew, or should have known, the importance of safeguarding Private Information

[30] https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing- attack.

entrusted to it by Plaintiffs and Class Members, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed Plaintiffs and Class Members as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

Value Of Private Information

88. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[31] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[32]

89. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[33]

90. For example, PII can be sold at a price ranging from $40 to $200.[34] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[35]

70. Moreover, Social Security numbers are among the worst kinds of Private Information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

---

[31] 17 C.F.R. § 248.201 (2013).
[32] *Id.*
[33] https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/
[34] https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/
[35] https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/

71. According to the Social Security Administration, each time an individual's Social Security number is compromised, "the potential for a thief to illegitimately gain access to bank accounts, credit cards, driving records, tax and employment histories and other private information increases."[36] Moreover, "[b]ecause many organizations still use SSNs as the primary identifier, exposure to identity theft and fraud remains."[37]

72. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiffs and some Class Members, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[38]

73. In fact, "[a] stolen Social Security number is one of the leading causes of identity theft and can threaten your financial health."[39] "Someone who has your SSN can use it to impersonate you, obtain credit and open bank accounts, apply for jobs, steal your tax refunds, get medical treatment, and steal your government benefits."[40]

74. What's more, it is no 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. In other words, preventive action to defend against the possibility of

[36] https://www.ssa.gov/phila/ProtectingSSNs.htm#:~:text=An%20organization's%20collection%20and%20use,and%20other%20private%20information%20increases.
[37] *Id.*
[38] https://www.ssa.gov/pubs/EN-05-10064.pdf
[39] https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft/
[40] https://www.investopedia.com/terms/s/ssn.asp.

misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

75. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[41]

76. For these reasons, some courts have referred to Social Security numbers as the "gold standard" for identity theft. *Portier v. NEO Tech. Sols*., No. 3:17-CV-30111, 2019 WL 7946103, at *12 (D. Mass. Dec. 31, 2019) ("Because Social Security numbers are the gold standard for identity theft, their theft is significant . . . . Access to Social Security numbers causes long-lasting jeopardy because the Social Security Administration does not normally replace Social Security numbers."), report and recommendation adopted, No. 3:17-CV-30111, 2020 WL 877035 (D. Mass. Jan. 30, 2020); *see also McFarlane v. Altice USA, Inc*., 2021 WL 860584, at *4 (citations omitted) (S.D.N.Y. Mar. 8, 2021) (the court noted that Plaintiff' Social Security numbers are: arguably "the most dangerous type of personal information in the hands of identity thieves" because it is immutable and can be used to "impersonat[e] [the victim] to get medical services, government benefits, ... tax refunds, [and] employment." . . . Unlike a credit card number, which can be changed to eliminate the risk of harm following a data breach, "[a] social security number derives its value in that it is immutable," and when it is stolen it can "forever be wielded to identify [the victim] and target him in fraudulent schemes and identity theft attacks.")

77. Similarly, the California state government warns consumers that: "[o]riginally, your Social Security number (SSN) was a way for the government to track your earnings and pay

[41] http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft.

you retirement benefits. But over the years, it has become much more than that. It is the key to a lot of your personal information. With your name and SSN, an identity thief could open new credit and bank accounts, rent an apartment, or even get a job."[42]

78. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[43]

79. The greater efficiency of electronic health records brings the risk of privacy breaches. These electronic health records contain a lot of sensitive information (*e.g.,* patient data, patient diagnosis, lab results, medications, prescriptions, treatment plans, etc.) that is valuable to cybercriminals. One patient's complete record can be sold for hundreds of dollars on the dark web. As such, PHI/PII is a valuable commodity for which a "cyber black market" exists where criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites. Unsurprisingly, the healthcare industry is at high risk and is acutely affected by cyberattacks, like the Data Breach here.

80. Between 2005 and 2019, at least 249 million people were affected by healthcare data breaches.[44] Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.[45] In short, these sorts of data breaches are increasingly common, especially among healthcare systems, which account for 30.03 percent of overall health data breaches, according to cybersecurity firm Tenable.[46]

---

[42] https://oag.ca.gov/idtheft/facts/your-ssn.
[43] https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected
[44] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/
[45] https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/
[46] https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-incovid-19-era-breaches/

81. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[47]

82. A study by Experian found that the average cost of medical identity theft is "about $20,000" per incident and that most victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive to restore coverage.[48] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third of medical identity theft victims saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.[49]

83. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—dates of birth, names, Social Security numbers, and medical information.

84. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[50]

85. Among other forms of fraud, identity thieves may obtain driver's licenses,

[47] https://khn.org/news/rise-of-indentity-theft/
[48] https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/
[49] *Id.; see also* https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-toknow-about-them-and-what-to-do-after-one/
[50] https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html

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

86. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[51]

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

Defendant Fails To Comply With FTC Guidelines

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

89. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[52]

[51] *available at:* https://www.gao.gov/assets/gao-07-737.pdf
[52] https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf

90. 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.[53]

91. The FTC further recommends that companies not maintain Private Information 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.

92. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential patient 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.

93. 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. (Henry Ford) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

94. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice

[53] *Id.*

by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

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

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

97. Upon information and belief, TRA was at all times fully aware of its obligation to protect the Private Information of its patients, TRA was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

Defendant Fails To Comply With HIPAA Guidelines

98. Defendant is a covered entity under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

99. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[54] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

[54] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

100. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

101. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

102. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

103. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

104. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

105. HIPAA also requires Defendant to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendant is

required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

106. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

107. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[55]

108. HIPAA requires a covered entity to have and apply appropriate sanctions against patients of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

109. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

110. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed

[55] https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e- and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material.[56] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-." US Department of Health & Human Services, Guidance on Risk Analysis.[57]

Defendant Fails To Comply With Industry Standards

111. As noted above, experts studying cyber security routinely identify healthcare entities in possession of Private Information as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

112. Several best practices have been identified that, at a minimum, should be implemented by healthcare entities in possession of Private Information, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. TRA failed to follow these industry best practices, including a failure to implement multi-factor authentication.

113. Other best cybersecurity practices that are standard for healthcare entities 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

[56] http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html.
[57] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. TRA failed to follow these cybersecurity best practices, including failure to train staff.

114. Defendant failed to meet the minimum standards of one or more of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

115. These foregoing frameworks are existing and applicable industry standards for healthcare entities, and upon information and belief, Defendant failed to comply with at least one––or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

Common Injuries & Damages

116. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) 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.

Data Breaches Increase Victims' Risk Of Identity Theft

117. The unencrypted Private Information of Class Members is already for sale on the dark web as that is the *modus operandi* of hackers.

118. Unencrypted Private Information may also fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiffs and Class Members. Simply put, unauthorized individuals can easily access the Private Information of Plaintiffs and Class Members.

119. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

122. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity – or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

123. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to

manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

124. The Dark Web is an unindexed layer of the internet that requires special software or authentication to access.[58] Criminals in particular favor the Dark Web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or 'surface' web, Dark Web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the Dark Web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[59] This prevents Dark Web marketplaces from being easily monitored by authorities or accessed by those not in the know.

125. A sophisticated black market exists on the Dark Web where criminals can buy or sell malware, firearms, drugs, and frequently, personal and medical information like the PII and PHI at issue here.[60] The digital character of PII stolen in data breaches lends itself to Dark Web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information.[61] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[62]

120. As extensively explained above, Plaintiffs' and Class Members' Private

[58] https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.
[59] *Id*.
[60] https://www.microsoft.com/en- us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.
[61] *Id*.; https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.
[62] https://www.microsoft.com/en- us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.

Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiffs and Class Members and to profit off their misfortune.

123. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[63]

124. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

125. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

126. The existence and prevalence of "Fullz" packages means that the Private

[63] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/

Information stolen from the data breach can easily be linked to the unregulated data (like contact information) of Plaintiffs and the other Class Members.

127. Thus, even if certain information (such as contact information) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

128. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss Of Time To Mitigate Risk Of Identity Theft & Fraud

129. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their Private Information was compromised, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

130. Plaintiffs and Class Members' Private Information is already available on the dark web and therefore they must take extensive steps in order to protect themselves from identity theft and/or fraud which requires significant time that Plaintiffs and Class Members must undertake in response to the Data Breach. Plaintiffs' and Class Members' time is highly valuable and irreplaceable, and accordingly, Plaintiffs and Class Members suffered actual injury and damages in the form of lost time that they spent on mitigation activities in response to the Data Breach.

131. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach as well as changing passwords and resecuring their own computer networks. Accordingly,

the Data Breach has caused Plaintiffs and Class Members to suffer actual injury in the form of lost time—which cannot be recaptured—spent on mitigation activities.

132. Plaintiffs' mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[64]

133. Plaintiffs' mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[65]

134. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[66]

Diminution of Value of Private Information

135. As extensively stated above, PII and PHI are valuable property rights. Their value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

[64] https://www.gao.gov/new.items/d07737.pdf.
[65] https://www.identitytheft.gov/Steps
[66] https://www.gao.gov/new.items/d07737.pdf

136. An active and robust legitimate marketplace for PHI also exists. In 2019, the data brokering industry was worth roughly $200 billion.[67]

137. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

138. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

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

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

141. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to, upon information and belief, thousands to tens of thousands of individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

[67] https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/

142. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

143. Given the type of targeted attack in this case, sophisticated criminal activity, and the type of Private Information involved, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes –*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

144. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Private Information 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.

145. Consequently, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

146. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach.

Loss Of Benefit Of The Bargain

147. Furthermore, Defendant's poor data security practices deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to pay Defendant and/or its agents for the

provision of medical services, Plaintiffs and other reasonable patients understood and expected that they were, in part, paying for the services and necessary data security to protect the Private Information, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

Plaintiff Norma Covey's Experience

148. Plaintiff Covey provided her Private Information to Defendant as a condition of receiving healthcare services from Defendant which was then entered into Defendant's computer system and maintained by Defendant at the time of the Data Breach.

149. Plaintiff Covey reasonably understood and expected that Defendant would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff Covey would not have allowed Defendant, or anyone in Defendant's position, to maintain her Private Information if she believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

150. Plaintiff Covey received a Notice letter, dated July 12, 2024, from Defendant informing her that her Private Information had been compromised in the Data Breach. The Notice letter stated that Plaintiff Covey's full name, Social Security number, address, gender, date of birth, medical record number, phone number, health insurance information, prescription information, medical appointment information, clinical information, scanned documents and/or images, and email address was accessed in the Data Breach.

151. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Covey faces, Defendant offered her a twelve-month subscription to a credit monitoring service. The Notice letter Plaintiff Covey received also cautioned her to "to remain vigilant against

incidents of identity theft and fraud by reviewing your account statements, explanation of benefits forms, and monitoring your free credit reports for suspicious activity."

152. Plaintiff Covey greatly values her privacy and Private Information and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Covey is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

153. Plaintiff Covey stores any and all documents containing Private Information in a secure location and destroys any documents she receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise her identity and credit card accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

154. To Plaintiff Covey's knowledge, her Private Information has not been compromised in a prior data breach.

155. As a result of the Data Breach, Plaintiff Covey has spent approximately 3-4 hours on activities including researching and verifying the legitimacy of the Data Breach, blocking spam callers, and monitoring her financial accounts for unusual activity, which may take years to detect, and other necessary mitigation efforts. This is valuable time that Plaintiff spent at Defendant's direction and that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

156. As a consequence of and following the Data Breach, Plaintiff Covey has experienced an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach. This misuse of her Private Information was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information

compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud. Upon information and belief, both fraudulent transactions were a result of the Data Breach.

157. Plaintiff Covey additionally suffered actual injury in the form of fraudulent charges on her debit card. On or about May 2024 Plaintiff became aware of two separate unauthorized transactions on her debit card. One transaction was from Walmart.com for $351.01. The second transaction was from approximately $40.00.

158. The Data Breach has caused Plaintiff Covey to suffer fear, anxiety, and stress, which has been compounded by Defendant's three-month delay in noticing her of the fact that her Social Security number in conjunction with her date of birth and other information was acquired by criminals as a result of the Data Breach.

159. Plaintiff Covey 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 Covey will continue to be at present and continued increased risk of identity theft and fraud for years to come.

160. Plaintiff Covey has a continuing interest in ensuring that her Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Lewis Benavides's Experience

161. Plaintiff Benavides provided his Private Information to Defendant as a condition of

receiving healthcare services from Defendant which was then entered into Defendant's computer system and maintained by Defendant at the time of the Data Breach.

162. Plaintiff Benavides reasonably understood and expected that Defendant would safeguard his Private Information and timely and adequately notify him in the event of a data breach. Plaintiff Benavides would not have allowed Defendant, or anyone in Defendant's position, to maintain his Private Information if he believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

163. Plaintiff Benavides received a Notice letter dated July 12, 2024, from Defendant informing him that his Private Information had been compromised in the Data Breach. The Notice letter stated that Plaintiff Benavides' name, Social Security Number, address, gender, date of birth, medical record number, phone number, health insurance information, prescription information, medical appointment information, clinical information, scanned documents and/or images, and email address were accessed in the Data Breach.

164. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Benavides faces, Defendant offered him a twelve-month subscription to a credit monitoring service. The Notice letter Plaintiff Benavides received also cautioned him to "to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, explanation of benefits forms, and monitoring your free credit reports for suspicious activity."

165. Plaintiff Benavides greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Benavides is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

166. Plaintiff Benavides stores any and all documents containing Private Information in

a secure location and destroys any documents he receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise his identity and credit card accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

167. As a result of the Data Breach, Plaintiff Benavides has spent approximately two hours reviewing his credit reports, changing compromised passwords of his bank accounts, and other necessary mitigation efforts. This is valuable time that Plaintiff spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

168. As a consequence of and following the Data Breach, Plaintiff Benavides has experienced alerts that his personal information such as his Social Security number was on the Dark Web, that his bank account passwords were compromised, has experienced an increase in spams call and text messages, and received an alert that an individual attempted to hack into his American Airlines Advantage account and transfer miles to another account.

169. The Data Breach has caused Plaintiff Benavides to suffer fear, anxiety, and stress, which has been compounded by Defendant's three-month delay in noticing him of the fact that his Social Security number in conjunction with his date of birth and other information was acquired by criminals as a result of the Data Breach.

170. Plaintiff Benavides anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. In addition, Plaintiff Benavides will continue to be at present and continued increased risk of identity theft and fraud for years to come.

171. Indeed, shortly following the Data Breach, Plaintiff Benavides was alerted that his

Private Information, including at least his Social Security Number, was discovered on the dark web for access and exploitation by cybercriminals.

172. Plaintiff Benavides has a continuing interest in ensuring that his Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Robert Leigh-Manuell's Experience

173. Plaintiff Leigh-Manuell provided his Private Information to Defendant as a condition of receiving healthcare services from Defendant which was then entered into Defendant's computer system and maintained by Defendant at the time of the Data Breach.

174. Plaintiff Leigh-Manuell reasonably understood and expected that Defendant would safeguard his Private Information and timely and adequately notify him in the event of a data breach. Plaintiff Leigh-Manuell would not have allowed Defendant, or anyone in Defendant's position, to maintain his Private Information if he believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access. Upon information and belief, Plaintiff Leigh-Manuell is a data breach victim.

175. Plaintiff Leigh-Manuell greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Leigh-Manuell is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

176. Plaintiff Leigh-Manuell stores any and all documents containing Private Information in a secure location and destroys any documents he receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise his identity and credit card accounts. Moreover, he diligently chooses unique

usernames and passwords for his various online accounts.

177. To Plaintiff Leigh-Manuell's knowledge, his Private Information has not been compromised in a prior data breach.

178. As a result of the Data Breach, Plaintiff Leigh-Manuell has spent approximately 2 hours per week since learning of the Breach on activities including researching and verifying the legitimacy of the Data Breach, blocking spam callers, and monitoring his financial accounts for unusual activity, which may take years to detect, and other necessary mitigation efforts. This is valuable time that Plaintiff spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

179. The Data Breach has caused Plaintiff Leigh-Manuell to suffer fear, anxiety, and stress, which has been compounded by Defendant's delay in noticing him of the fact that his Social Security number in conjunction with his date of birth and other information was acquired by criminals as a result of the Data Breach.

180. Plaintiff 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 will continue to be at present and continued increased risk of identity theft and fraud for years to come.

181. Plaintiff Leigh-Manuell has a continuing interest in ensuring that his Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff David Hickey's Experience

182. Plaintiff Hickey is a current patient of Defendant and provided his Private Information to Defendant as a condition of receiving healthcare services. His Private Information was then entered into Defendant's computer system and maintained by Defendant at the time of

the Data Breach.

183. Plaintiff Hickey reasonably understood and expected that Defendant would safeguard his Private Information and timely and adequately notify him in the event of a data breach. Plaintiff Hickey would not have allowed Defendant, or anyone in Defendant's position, to maintain his Private Information if he believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

184. Plaintiff Hickey received a Notice letter dated July 12, 2024, from Defendant informing him that his Private Information had been compromised in the Data Breach. The Notice letter stated that Plaintiff Hickey' name, Social Security Number, address, gender, date of birth, medical record number, phone number, health insurance information, prescription information, medical appointment information, clinical information, scanned documents and/or images, and email address were accessed in the Data Breach.

185. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Hickey faces, Defendant offered him a twelve-month subscription to a credit monitoring service. The Notice letter Plaintiff Hickey received also cautioned him to "to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, explanation of benefits forms, and monitoring your free credit reports for suspicious activity."

186. Plaintiff Hickey greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Hickey is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

187. Plaintiff Hickey stores any and all documents containing Private Information in a secure location and destroys any documents he receives in the mail that contain any Private

Information or that may contain any information that could otherwise be used to compromise his identity and credit card accounts.

188. As a result of the Data Breach, Plaintiff Hickey has spent at least five hours reviewing his credit reports, changing compromised passwords of his bank accounts, signing up for credit monitoring services, and engaging in other necessary mitigation efforts. This is valuable time that Plaintiff spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

189. The Data Breach has caused Plaintiff Hickey to suffer fear, anxiety, and stress, which has been compounded by Defendant's three-month delay in noticing him of the fact that his Social Security number in conjunction with his date of birth and other information, including medical and clinical information, was acquired by criminals as a result of the Data Breach.

190. Plaintiff Hickey anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. In addition, Plaintiff Hickey will continue to be at present and continued increased risk of identity theft and fraud for years to come.

191. Plaintiff Hickey has a continuing interest in ensuring that his Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Mark Bennett's Experience

192. Plaintiff Mark Bennett is and at all times mentioned herein was an individual citizen

193. residing in the State of Texas, in the city of Denison.

194. Plaintiff Bennett was a patient at TRA.

195. After Plaintiff Bennett provided Private Information, Defendant suffered a Data

Breach.

196. Plaintiff Bennett was a patient of TRA before the Data Breach.

197. When Plaintiff Bennett received his Notice Letter, sent July 12, the letter stated that his PII and PHI may have been either accessed and/or acquired by an unauthorized individual including Plaintiff Bennett's "name, Social Security number, address, gender, date of birth, medical record number, phone number, health insurance information, prescription information, medical appointment information, clinical information, scanned documents and/ or images, and email address." Exhibit A.

198. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Bennett faces, Defendant offered him a twelve-month subscription to a credit monitoring service. The Notice letter Plaintiff Bennett received also cautioned him to "to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, explanation of benefits forms, and monitoring your free credit reports for suspicious activity."

199. Plaintiff Bennett is especially alarmed by the amount of stolen or accessed PII and PHI listed on his letter. Despite Defendant providing that list, he cannot be sure more of his PII or PHI was exfiltrated. Now he checks his bank accounts and credit cards throughout the day each day, spending approximately an hour per week just monitoring accounts because of Defendant's Data Breach.

200. Plaintiff Bennett knows that cybercriminals often sell Private Information, and that his PII or PHI could be abused for months or even years after a data breach. Had Plaintiff Bennett been aware that Defendant's computer systems were not secure, he would not have entrusted Defendant with his personal data.

201. Plaintiff Bennett anticipates spending considerable time and money on an ongoing

basis to try to mitigate and address the harms caused by the Data Breach. In addition, Plaintiff Hickey will continue to be at present and continued increased risk of identity theft and fraud for years to come.

202. Plaintiff Bennett has a continuing interest in ensuring that his Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

203. Pursuant to Rule 42 of the Texas Rules of Civil Procedure, Plaintiffs propose the following Class definition, subject to amendment as appropriate:

> All individuals whose Private Information was accessed and/or acquired by an unauthorized party as a result of the data breach reported by Defendant in April 2024 (the "Class").

204. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family patients.

205. Plaintiffs reserve the right to amend the definitions of the Class or add a Class or Subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

206. Numerosity: The patients of the Class are so numerous that joinder of all patients is impracticable, if not completely impossible. Although the precise number of individuals is currently unknown to Plaintiffs and exclusively in the possession of Defendant, upon information and belief, 297,500 individuals' information was disclosed. The Class is apparently identifiable

within Defendant's records.

207. Common questions of law and fact exist as to all patients of the Class and predominate over any questions affecting solely individual patients of the Class. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class Members, including the following:

a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiffs and Class Members;

b. Whether Defendant had respective duties not to disclose the Private Information of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendant had respective duties not to use the Private Information of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiffs and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;

h. 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;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Plaintiffs and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct;

k. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

208. Typicality: Plaintiffs' claims are typical of those of the other patients of the Class because Plaintiffs, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other patient of the Class.

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

210. Adequacy: Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiffs seek no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action and data breach litigation, and Plaintiffs intend to prosecute this action vigorously.

211. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will

permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

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

213. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

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

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

216. Further, 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.

217. Likewise, particular issues under Rule 42(d)(1) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the Plaintiffs and the class 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;
e. Whether Defendant failed to take commercially reasonable steps to safeguard patient Private Information; and whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

CAUSES OF ACTION
COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)

218. Plaintiffs re-allege and incorporate by reference all preceding allegations, as if fully set forth herein.

219. Defendant requires its patients, including Plaintiffs and Class Members, to submit non-public Private Information in the ordinary course of providing its services.

220. Defendant gathered and stored the Private Information of Plaintiffs and Class Members as part of its business of soliciting its services to its patients, which solicitations and services affect commerce.

221. Plaintiffs and Class Members entrusted Defendant with their Private Information with the understanding that Defendant would safeguard their information.

222. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information were wrongfully disclosed.

223. By voluntarily undertaking and assuming the responsibility to collect and store this data, and in fact doing so, 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 property—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 which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

224. Defendant owed a duty of care to safeguard the Private Information due to the foreseeable risk of a data breach and the severe consequences that would result from its failure to

so safeguard the Private Information.

225. 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.

226. 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)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

227. For instance, HIPAA required Defendant to notify victims of the Breach within 60 days of the discovery of the Data Breach. Defendant has not notified Plaintiffs and the Class that unauthorized persons had accessed and acquired their private, protected, and personal information.

228. 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 adequately protected the Private Information.

229. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between TRA and Plaintiffs and Class Members. That special relationship arose because Plaintiffs and the Class entrusted TRA with their confidential Private Information, a necessary part of being patients at Defendant.

230. 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.

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

232. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former patients' Private Information it was no longer required to retain pursuant to regulations.

233. Moreover, Defendant had a duty to promptly and adequately notify Plaintiffs and the Class of the Data Breach.

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

235. Defendant breached its duties, pursuant to the FTC Act, HIPAA, and other applicable standards, and thus was 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. Allowing unauthorized access to Class Members' Private Information;

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

e. Failing to remove former patients' Private Information it was no longer required to retain pursuant to regulations, and

f. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

236. Defendant violated Section 5 of the FTC Act and HIPAA by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

237. Plaintiffs and Class Members are within the class of persons that the Texas Medical Records Privacy Act, Tex. Health & Safety Code § 181.001, *et seq.*, and Texas Business and Commercial Code §§ 521.052 and 521.053 were intended to protect.

238. Plaintiffs and Class Members were within the class of persons the Federal Trade Commission Act and HIPAA were intended to protect and the type of harm that resulted from the Data Breach was the type of harm that the statutes were intended to guard against.

239. Defendant's violation of Section 5 of the FTC Act and HIPAA constitutes negligence.

240. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

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

practices.

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

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

244. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiffs and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems or transmitted through third party systems.

245. 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.

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

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

248. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement

(Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

249. Defendant has admitted that the Private Information of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

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

251. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiffs and the Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. The Private Information of Plaintiffs and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

252. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of their Private Information consisting of an increase in spam calls, texts, and/or emails; (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.

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

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

255. 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.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiffs and the Class)

256. Plaintiffs re-allege and incorporates by reference all preceding allegations, as if fully set forth herein.

257. Pursuant to the Texas Medical Records Privacy Act, Tex. Health & Safety Code § 181.001, et seq. and Texas Business and Commercial Code §§ 521.052 and 521.053, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' confidential Private Information from disclosure.

258. Defendant had a duty to use reasonable security measures, particularly because some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" per the Texas Medical Records Privacy Act.

259. Defendant breached its duties to Plaintiffs and Class Members under the Federal

Trade Commission Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

260. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

261. But for Defendant's wrongful and negligent breach of their duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

262. The harm resulting from the Data Breach was the harm the Texas statutes referenced herein were intended to guard against and Plaintiffs and Class Members are within the class of persons the statute was intended to protect.

263. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

264. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT III
Breach Of Implied Contract
(On Behalf of Plaintiffs and the Class)

265. Plaintiffs re-allege and incorporates by reference all preceding allegations, as if fully set forth herein.

266. Plaintiffs and Class Members were required to deliver their Private Information to Defendant as part of the process of obtaining services at Defendant. Plaintiffs and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for services.

267. 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.

268. Defendant accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of providing services to Plaintiffs and Class Members.

269. Plaintiffs and the Class entrusted their Private Information to Defendant. In so doing, Plaintiffs and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen.

270. 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 FTC guidelines on data security) and were consistent with industry standards.

271. Implicit in the agreement between Plaintiffs and Class Members and the Defendant to provide Private Information, was the latter's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiffs and Class Members from unauthorized disclosure or uses, (f) retain the Private Information only under conditions that kept such information secure and confidential.

272. The mutual understanding and intent of Plaintiffs and Class Members on the one

hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.

273. On information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiffs and Class Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

274. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiffs' and Class Members' Private Information would remain protected.

275. Plaintiffs and Class Members paid money to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

276. 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.

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

278. Every contract in this State has an implied covenant of good faith and fair dealing, which is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

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

280. Defendant breached the implied contracts it made with Plaintiffs and the Class by

failing to safeguard and protect their personal information, by failing to delete the information of Plaintiffs and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

281. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard Private Information, failing to timely and accurately disclose the Data Breach to Plaintiffs and Class Members and continued acceptance of Private Information and storage of other personal information after Defendant knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

282. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiffs and Class Members sustained damages, including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of their Private Information consisting of an increase in spam calls, texts, and/or emails; (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.

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

284. 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 credit monitoring to all Class Members.

COUNT IV
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

285. Plaintiffs re-allege and incorporate by reference all preceding allegations, as if fully set forth herein.

286. In light of the special relationship between Defendant 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, (1) to act primarily for Plaintiffs and Class Members, (2) for the safeguarding of their Private Information; (3) to timely notify Plaintiffs and Class Members of a Data Breach's occurrence and disclosure; and (4) to maintain complete and accurate records of what information (and where) Defendant did and does store.

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

288. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members because of the high degree of trust and confidence inherent to the nature of the relationship between Plaintiffs and Class Members on the one hand and Defendant on the other, including with respect to their Private Information.

289. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing

to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

290. 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.

291. 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.

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

293. 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) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of their Private Information consisting of an increase in spam calls, texts, and/or emails; (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.

COUNT V
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

294. Plaintiffs re-allege and incorporate by reference all preceding allegations, as if fully set forth herein.

295. Plaintiffs bring this Count in the alternative to the breach of implied contract count above.

296. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they paid Defendant and/or its agents for services and in so doing also provided Defendant with their Private Information. In exchange, Plaintiffs and Class Members should have received from Defendant the services that were the subject of the transaction and should have had their Private Information protected with adequate data security.

297. Defendant knew that Plaintiffs and Class Members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the Private Information entrusted to it. Defendant profited from Plaintiffs' retained data and used Plaintiffs' and Class Members' Private Information for business purposes.

298. Defendant failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not fully compensate Plaintiffs or Class Members for the value that their Private Information provided.

299. Defendant acquired the Private Information through inequitable record retention as it failed to investigate and/or disclose the inadequate data security practices previously alleged.

300. If Plaintiffs and Class Members had known that Defendant would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their Private Information, they would have entrusted their Private Information at Defendant or obtained services at Defendant.

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

302. Defendant 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 hacking incident, Defendant instead calculated to increase its own profit at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

303. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiffs and Class Members conferred upon it.

304. 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) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of their Private Information consisting of an increase in spam calls, texts, and/or emails; (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.

305. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or

damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

306. Plaintiffs and Class Members may not have an adequate remedy at law against Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT VI
Invasion of Privacy (Public Disclosure of Private Facts)
(On behalf of Plaintiffs and the Class)

307. Plaintiffs re-allege and incorporate by reference all preceding allegations, as if fully set forth herein.

308. Plaintiffs and Class Members had a reasonable expectation of privacy in the Private Information Defendant mishandled.

309. As a result of Defendant's conduct, publicity was given to Plaintiffs' and Class Members' Private Information, which necessarily includes matters concerning their private life such as their Private Information.

310. A reasonable person of ordinary sensibilities would consider the publication of Plaintiffs' and Class Members' Private Information to be highly offensive.

311. Plaintiffs' and Class Members' Private Information is not of legitimate public concern and should remain private.

312. As such, Defendant's conduct, as alleged above, resulted in a public disclosure of private facts, for which it is liable.

313. As a direct and proximate result of Defendant's publication of their private facts,

Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial and any other relief allowed by law.

COUNT VII
Declaratory Judgment/Injunctive Relief
(On behalf of Plaintiffs and the Class)

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

315. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard Plaintiffs' and Class Members' Private Information, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from future data breaches that compromise their Private Information. Plaintiffs and the Class remain at imminent risk that further compromises of their Private Information will occur in the future.

316. The Court should also issue prospective injunctive relief requiring Defendant to employ adequate security practices consistent with law and industry standards to protect employee and patient Private Information.

317. Defendant still possesses the Private Information of Plaintiffs and the Class.

318. To Plaintiffs' knowledge, Defendant has made no announcement that it has changed its data storage or security practices relating to the Private Information.

319. To Plaintiffs' knowledge, Defendant has made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

320. If an injunction is not issued, Plaintiffs and the Class 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.

321. As described above, actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiffs and Class Members. Further, Plaintiffs and Class Members are at risk of additional or further harm due to the exposure of their Private Information and Defendant's failure to address the security failings that led to such exposure.

322. There is no reason to believe that Defendant's employee training and security measures are any more adequate now than they were before the breach to meet Defendant's contractual obligations and legal duties.

323. 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 data breach occurs at Defendant, Plaintiffs and Class Members will likely continue to 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 a pre-existing legal obligation to employ such measures.

324. Issuance of the requested injunction will not disserve 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 Class.

325. Plaintiffs and Class Members, therefore, seek a declaration (1) that Defendant's existing data security measures do not comply with its contractual obligations and duties of care to provide adequate data security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Ordering that Defendant engage internal security personnel to conduct testing, including audits on Defendant's systems, on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train its security personnel and employees regarding any new or modified data security policies and procedures;

d. Ordering that Defendant purge, delete, and destroy, in a reasonably secure manner, any Private Information not necessary for its provision of services;

e. Ordering that Defendant conduct regular database scanning and security checks; and

f. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information, including but not limited to, client personally identifiable information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, requests judgment against Defendant and that the Court grants the following:

A. For an Order certifying the Class, 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 the Private

Information of Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendant to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information for Plaintiffs' and Class Members' respective lifetimes;

v. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiffs and Class Members;

vi. prohibiting Defendant from maintaining the Private Information of Plaintiffs and Class Members on a cloud-based database;

vii. requiring Defendant to engage independent third-party security

auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

viii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

ix. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

x. requiring Defendant to segment data by, among other things, creating firewalls and controls so that if one area of Defendant's network is compromised, hackers cannot gain access to portions of Defendant's systems;

xi. requiring Defendant to conduct regular database scanning and securing checks;

xii. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xiii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiv. requiring Defendant to implement a system of tests to assess its respective

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

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

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

xvii. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xviii. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, nominal, statutory, consequential, and punitive damages, as allowed by law in an amount to be determined;

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

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

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

Dated: September 27, 2024

Respectfully Submitted,

/s/ *Joe Kendall*
JOE KENDALL
Texas Bar No. 11260700
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Suite 825
Dallas, Texas 75219
214-744-3000
214-744-3015 (Facsimile)
jkendall@kendalllawgroup.com

Raina Borrelli*
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, IL 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
raina@straussborrelli.com

John J. Nelson*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
402 W. Broadway, Suite 1760
San Diego, CA 92101
Telephone: (858) 209-6941
jnelson@milberg.com

Charles Schaffer*
LEVIN, SEDRAN & BERMAN LLP
510 Walnut Street, Suite 500
Philadelphia, Pennsylvania 19106
Phone: 215- 592-1500
cschaffer@lfsblaw.com

M. Anderson Berry*
Gregory Haroutunian*
Andrew Snyder (Texas Bar No. 24102997)

CLAYEO C. ARNOLD
A PROFESSIONAL CORPORATION
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Fax: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com
asnyder@justice4you.com

Jeffrey S. Goldenberg*
GOLDENBERG SCHNEIDER, LPA
4445 Lake Forest Drive, Suite 490
Cincinnati, Ohio 45242
Phone: 513-345-8291
Fax: 513-345-8294
jgoldenberg@gs-legal.com

Brett R. Cohen*
LEEDS BROWN LAW, P.C.
One Old Country Road - Suite 347
Carle Place, New York 11514
Phone: 516-874-4505
bcohen@leedsbrownlaw.com

Tyler Bean*
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, NY 10151
Telephone: 929-677-5144
tbean@sirillp.com

Jarrett L. Ellzey
Leigh S. Montgomery
ELLZEY, KHERKHER, SANFORD & MONTGOMERY, LLP
4200 Montrose, Ste. 200
Houston, Texas 77995
Telephone: (713) 554-2377
jellzey@eksm.com
lmontgomery@eksm.com

* (*Pro Hac Vice forthcoming)*

Attorneys for Plaintiffs and the Proposed Class

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing document was served on all counsel of record on September 27, 2024 via e-file Texas, in accordance with the Texas Rules of Civil Procedure.

/s/ *Joe Kendall*
Joe Kendall

Automated Certificate of eService

This automated certificate of service was created by the efiling system. The filer served this document via email generated by the efiling system on the date and to the persons listed below. The rules governing certificates of service have not changed. Filers must still provide a certificate of service that complies with all applicable rules.

Joe Kendall
Bar No. 11260700
administrator@kendalllawgroup.com
Envelope ID: 92534582
Filing Code Description: Amended Petition
Filing Description: PLAINTIFFS' CONSOLIDATED CLASS ACTION PETITION
Status as of 9/27/2024 1:55 PM CST

Associated Case Party: NORMA COVEY

Name	BarNumber	Email	TimestampSubmitted	Status
joe kendall		jkendall@kendalllawgroup.com	9/27/2024 11:59:55 AM	SENT

Associated Case Party: TEXAS RETINA ASSOCIATES

Name	BarNumber	Email	TimestampSubmitted	Status
Meghan McCaig		meghan.mccaig@hklaw.com	9/27/2024 11:59:55 AM	SENT

Case Contacts

Name	BarNumber	Email	TimestampSubmitted	Status
John Nelson		jnelson@milberg.com	9/27/2024 11:59:55 AM	SENT
Raina Borrelli		raina@straussborrelli.com	9/27/2024 11:59:55 AM	SENT
Charles Schaffer		cschaffer@lfsblaw.com	9/27/2024 11:59:55 AM	SENT
Jeffery Goldenberg		jgoldenberg@gs-legal.com	9/27/2024 11:59:55 AM	SENT
Brett Cohen		bcohen@leedsbrownlaw.com	9/27/2024 11:59:55 AM	SENT
M. AndersonBerry		aberry@justice4you.com	9/27/2024 11:59:55 AM	SENT
Wanda Sneed		wanda.sneed@hklaw.com	9/27/2024 11:59:55 AM	SENT
Angelea Boots		angelea@justice4you.com	9/27/2024 11:59:55 AM	SENT
Andrew Snyder		asnyder@justice4you.com	9/27/2024 11:59:55 AM	SENT