IN THE CIRCUIT COURT OF THE ELEVENTH JUDICIAL CIRCUIT
IN AND FOR MIAMI DADE COUNTY, FLORIDA

| | |
|---|---|
| DOMINIC JARA, RAFAEL CHINCHILLA, LINDA SIMON, and BRENDA IRIBARREN, individually and on behalf of all others similarly situated,<br><br>Plaintiffs,<br><br>v.<br><br>SOUTH FLORIDA BEHAVIORAL HEALTH NETWORK INCORPORATED, d/b/a THRIVING MIND,<br><br>Defendant. | **CASE NO. 2024-010316-CA-01 (CA30)**<br><br>**Judge Reemberto Diaz**<br><br>**JURY TRIAL DEMANDED** |

# CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Dominic Jara, Rafael Chinchilla, Linda Simon, and Brenda Iribarren ("Plaintiffs") bring this Consolidated Class Action Complaint ("Complaint") against Defendant South Florida Behavioral Health Network Incorporated d/b/a Thriving Mind ("Thriving Mind" 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:

## NATURE OF THE ACTION

1. This Class Action arises from a cyberattack resulting in a data breach of sensitive information in the possession and custody and/or control of Defendant (the "Data Breach").

2. The Data Breach resulted in unauthorized disclosure, exfiltration, and theft of current and former patients' highly personal information, including name, Social Security number, date of birth, financial information ("personally identifying information" or "PII") medical

information and health insurance information ("protected health information" or "PHI"). Plaintiffs refer to both PII and PHI collectively as "Sensitive Information."

3. On information and belief, the Data Breach occurred between at least August 1, 2023, and August 3, 2023. Defendant did not discover the Breach until August 3, 2023, allowing cybercriminals unfettered access to Plaintiffs' and the Class's most sensitive information for at least three days.

4. On May 29, 2024, Thriving Mind finally notified state Attorneys General and many Class Members about the widespread Data Breach ("Notice Letter"). A sample Notice Letter is attached hereto as ***Exhibit A***. Thriving Mind waited an appalling *302 days* before informing Class Members even though Plaintiffs and at least 225,000 Class Members had their most sensitive personal information accessed, exfiltrated, and stolen, causing them to suffer ascertainable losses in the form of the loss of the benefit of their bargain and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

5. Thriving Mind's Breach Notice obfuscated the nature of the breach and the threat it posted—refusing to tell its patients how many people were impacted, how the breach happened, or why it took Thriving Mind 302 days to begin notifying victims that hackers had gained access to highly private Sensitive Information.

6. Defendant's failure to timely detect and report the Data Breach made its patients vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their Sensitive Information.

7. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII and PHI misuse.

8. In failing to adequately protect Plaintiffs' and the Class's Sensitive Information, failing to adequately notify them about the breach, and by obfuscating the nature of the breach, Defendant violated state and federal law and harmed thousands of its current and former patients.

9. Plaintiffs and members of the proposed Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiffs and members of the proposed Class trusted Defendant with their Sensitive Information. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

10. Plaintiffs are Thriving Mind Data Breach victims.

11. Accordingly, Plaintiffs, on their own behalfs, and on behalf of a class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendant's possession.

## PARTIES

12. Plaintiff Dominic Jara is a natural person and citizen of Miami-Dade County Florida, where he intends to remain.

13. Plaintiff Rafael Chinchilla is a natural person and citizen of Miami-Dade County Florida, where he intends to remain.

14. Plaintiff Linda Simon is a natural person and citizen of Monroe County, Florida, where she intends to remain.

15. Plaintiff Brenda Iribarren is a natural person and citizen of Miami-Dade County, Florida, where she intends to remain.

16. Defendant Thriving Mind is a Florida corporation with its headquarters and principal place of business located at 7205 NW 19th Street Miami, FL 33126.

## JURISDICTION AND VENUE

17. The Court has subject matter jurisdiction over Plaintiffs' claims under Florida Stat.§ 26.012 and § 86.011. This Court has jurisdiction over this dispute because this complaint seeks damages over $50,000.00, exclusive of interest and attorneys' fees.

18. The Court has personal jurisdiction over Defendant because under Florida Stat. § 48.193, Defendant personally or through its agents operated, conducted, engaged in, or carried on a business or business venture in Florida; had offices in Florida; committed tortious acts in Florida; and because Defendant engaged in significant business activity within Florida.

19. Venue is proper in Miami-Dade County under Florida Stat. § 47.011 and § 47.051 because Defendant is headquartered and does business in this county, the causes of action accrued in this county, and Defendant has an office for the transaction of its customary business in this county.

## STATEMENT OF FACTS

***Thriving Mind***

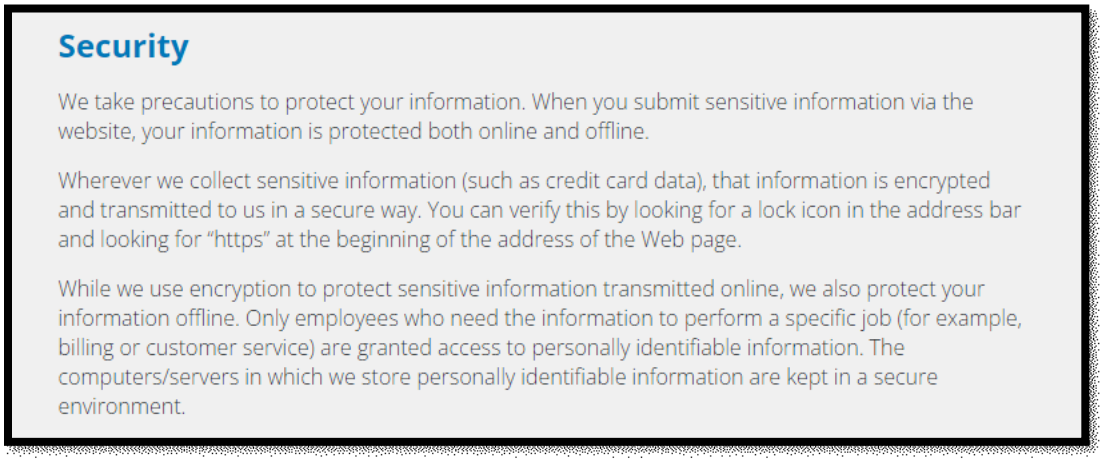
20. Thriving Mind is a Florida based healthcare facility that "promotes access to effective, accountable and compassionate care."[1] Thriving Mind boasts a total annual revenue of $130 million.[2]

21. As part of its business, Thriving Mind receives and maintains the Sensitive Information of thousands of current and former patients. In doing so, Thriving Mind implicitly promises to safeguard their Sensitive Information.

[1] Thriving Mind, About us, https://thrivingmind.org/ (last visited Oct. 23, 2024)
[2] Propublica, South Florida Behavioral Health Network, https://projects.propublica.org/nonprofits/organizations/593380599 (last visited Oct. 23, 2024)

22. In collecting and maintaining its current and former patients' Sensitive Information, Thriving Mind agreed it would safeguard the data in accordance with state and federal law. After all, Plaintiffs and Class Members themselves took reasonable steps to secure their Sensitive Information

23. Indeed, Defendant promises in its Privacy Policy that it "will not sell or rent this information to anyone."[3] Defendant further boasts that it takes a variety of precautions to protect patient information:



**Security**

We take precautions to protect your information. When you submit sensitive information via the website, your information is protected both online and offline.

Wherever we collect sensitive information (such as credit card data), that information is encrypted and transmitted to us in a secure way. You can verify this by looking for a lock icon in the address bar and looking for "https" at the beginning of the address of the Web page.

While we use encryption to protect sensitive information transmitted online, we also protect your information offline. Only employees who need the information to perform a specific job (for example, billing or customer service) are granted access to personally identifiable information. The computers/servers in which we store personally identifiable information are kept in a secure environment.

24. Despite recognizing its duty to do so, on information and belief, Thriving Mind has not implemented reasonably cybersecurity safeguards or policies to protect its patients' Sensitive Information or supervised its IT or data security agents and employees to prevent, detect, and stop breaches of its systems. As a result, Thriving Mind leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to patients' Sensitive Information.

***The Data Breach***

25. Plaintiffs were patients of Thriving Mind. As a condition of treatment with Thriving Mind, Plaintiffs provided Thriving Mind with their Sensitive Information, including but not limited to their names, Social Security numbers, and dates of birth. Thriving Mind used that Sensitive

[3] Thriving Mind, Privacy Policy, https://thrivingmind.org/legal (last visited Oct. 23, 2024)

Information to facilitate its treatment of Plaintiffs and required Plaintiffs to provide that Sensitive Information to obtain treatment and care.

26. On information and belief, Defendant collects and maintains patients' Sensitive Information in its computer systems.

27. In collecting and maintaining Sensitive Information, Defendant implicitly agrees that it will safeguard the data using reasonable means according to its internal policies as well as state and federal law.

28. According to the Breach Notice, on August 3, 2023, Thriving Mind discovered "suspicious activity on certain computer systems in our environment." Following an internal investigation, Thriving Mind admitted that "an unauthorized actor gained access to our servers between August 1 and August 3, 2023, and during this time certain internal files were obtained without authorization." Ex. A.

29. In other words, Thriving Mind's investigation revealed that its cyber and data security systems were completely inadequate and allowed cybercriminals to obtain files containing a treasure trove of thousands of its patients' highly private Sensitive Information.

30. Through its inadequate security practices, Defendant exposed Plaintiffs' and the Class's Sensitive Information for theft and sale on the dark web.

31. On or around May 29, 2024—302 days after the Breach first occurred– Thriving Mind finally began notifying Plaintiffs and Class Members about the Data Breach.

32. Despite its duties and alleged commitments to safeguard Sensitive Information, Defendant did not in fact follow industry standard practices in securing patients' Sensitive Information, as evidenced by the Data Breach.

33. In response to the Data Breach, Thriving Mind contends that it is "further enhancing our network security through the use of additional security tools and protocols." Ex. A. Although Defendant fails to expand on what these "enhancements" are, such enhancements should have been in place before the Data Breach. Ex. A.

34. Through the Data Breach, Defendant recognized its duty to implement reasonable cybersecurity safeguards or policies to protect patients Sensitive Information, insisting that, despite the Data Breach demonstrating otherwise, "[t]he privacy and security of information in our possession is one of our highest priorities" and that it "remain[s] dedicated to protecting the information in [its] care." Ex. A.

35. Through its Breach Notice, Defendant also recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to "remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits statements and monitoring your free credit reports for suspicious activity and to detect errors." Ex. A.

36. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiffs' and the Class's Sensitive Information. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiffs' and the Class's financial accounts.

37. On information and belief, Thriving Mind 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 Sensitive Information that cannot be changed, such as Social Security numbers.

38. Even with several months' worth of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiffs' and Class Members' Sensitive Information is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

39. On information and belief, Defendant failed to adequately train and supervise its IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its patients' Sensitive Information. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the Sensitive Information.

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

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

41. In light of recent high profile data breaches at other healthcare and healthcare adjacent companies, Defendant knew or should have known that its electronic records and patients' Sensitive Information would be targeted by cybercriminals.

42. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[4] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[5]

[4] 2021 Data Breach Annual Report, ITRC, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (last visited Oct. 23, 2023).

[5] *Id*.

43. Indeed, cyberattacks against the healthcare industry have become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime." [6]

44. Cyberattacks on medical systems and healthcare and healthcare adjacent companies like Defendant have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[7]

45. In fact, many high-profile ransomware attacks have occurred in healthcare and healthcare adjacent companies, with an estimated that nearly half of all ransomware attacks being carried out are on healthcare companies, and with 85% of those attacks being ransomware similar to the one occurring here.[8]

46. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Thriving Mind.

***Plaintiffs' Experiences***

[6] Gordon M. Snow Statement, FBI https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited March 13, 2023).
[7] Secret Service Warn of Targeted, Law360, https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited March 13, 2023).
[8] Ransomware explained, CSO, https://www.csoonline.com/article/563507/what-is-ransomware-how-it-works-and-how-to-remove-it.html (last visited Oct. 23, 2023).

**Plaintiff Dominic Jara**

47. Plaintiff Dominic Jara is a former Thriving Mind patient.

48. As a condition of treatment with Thriving Mind, Plaintiff provided it with his Sensitive Information, which Thriving Mind used to facilitate its treatment of Plaintiff and required Plaintiff to provide that Sensitive Information to obtain treatment and care.

49. Plaintiff provided his Sensitive Information to Defendant and trusted that it would use reasonable measures to protect it according to its internal policies as well as state and federal law.

50. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's Sensitive Information for theft by cybercriminals and sale on the dark web.

51. Plaintiff does not recall ever learning that his Sensitive Information was compromised in a data breach incident, other than the breach at issue in this case.

52. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

53. Indeed, as a result of this Data Breach, Plaintiff was forced to spend several hours placing a credit freeze.

54. Plaintiff has and will spend considerable time and effort monitoring his accounts to protect himself from additional identity theft. Plaintiff fears for his personal financial security and uncertainty over what Sensitive Information was exposed in the Data Breach.

55. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere

worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

56. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's Sensitive Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

57. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his Sensitive Information being placed in the hands of unauthorized third parties and possibly criminals.

58. Plaintiff suffered actual injury from the exposure and theft of his Sensitive Information—which violates his rights to privacy.

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

**Plaintiff Rafael Chinchilla**

60. Plaintiff Rafael Chinchilla is a former Thriving Mind patient.

61. As a condition of treatment with Thriving Mind, Plaintiff provided it with his Sensitive Information, which Thriving Mind used to facilitate its treatment of Plaintiff and required Plaintiff to provide that Sensitive Information to obtain treatment and care.

62. Plaintiff provided his Sensitive Information to Defendant and trusted that it would use reasonable measures to protect it according to its internal policies as well as state and federal law.

63. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's Sensitive Information for theft by cybercriminals and sale on the dark web.

64. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring his accounts to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

65. Plaintiff has and will spend considerable time and effort monitoring his accounts to protect himself from additional identity theft. Plaintiff fears for his personal financial security and uncertainty over what Sensitive Information was exposed in the Data Breach.

66. Plaintiff has and is experiencing feelings of anxiety, stress, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

67. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's Sensitive Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

68. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his Sensitive Information being placed in the hands of unauthorized third parties and possibly criminals.

69. Plaintiff suffered actual injury from the exposure and theft of his Sensitive Information—which violates his rights to privacy.

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

**Plaintiff Linda Simon**

71. Plaintiff Linda Simon is a former Thriving Mind patient. On or about May 29, 2024, she received a Notice Letter informing her that her Sensitive Information was involved in the Data Breach.

72. As a condition of treatment with Thriving Mind, Plaintiff provided it with her Sensitive Information, which Thriving Mind used to facilitate its treatment of Plaintiff and required Plaintiff to provide that Sensitive Information to obtain treatment and care.

73. Plaintiff provided her Sensitive Information to Defendant and trusted that it would use reasonable measures to protect it according to its internal policies as well as state and federal law.

74. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's Sensitive Information for theft by cybercriminals and sale on the dark web.

75. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring her accounts to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

76. Plaintiff has and will spend considerable time and effort monitoring her accounts to protect herself from additional identity theft. Plaintiff fears for her personal financial security and uncertainty over what Sensitive Information was exposed in the Data Breach.

77. Plaintiff has and is experiencing feelings of anxiety, stress, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience;

it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

78. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's Sensitive Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

79. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Sensitive Information being placed in the hands of unauthorized third parties and possibly criminals.

80. Plaintiff suffered actual injury from the exposure and theft of her Sensitive Information—which violates her rights to privacy.

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

**Plaintiff Brenda Iribarren**

82. Plaintiff Brenda Iribarren is a former Thriving Mind patient. On or about May 29, 2024, she received a Notice Letter informing her that her Sensitive Information was involved in the Data Breach.

83. As a condition of treatment with Thriving Mind, Plaintiff provided it with her Sensitive Information, which Thriving Mind used to facilitate its treatment of Plaintiff and required Plaintiff to provide that Sensitive Information to obtain treatment and care.

84. Plaintiff provided her Sensitive Information to Defendant and trusted that it would use reasonable measures to protect it according to its internal policies as well as state and federal law.

85. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's Sensitive Information for theft by cybercriminals and sale on the dark web.

86. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring her accounts to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

87. Plaintiff has and will spend considerable time and effort monitoring her accounts to protect herself from additional identity theft. Plaintiff fears for her personal financial security and uncertainty over what Sensitive Information was exposed in the Data Breach.

88. Plaintiff has and is experiencing feelings of anxiety, stress, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

89. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's Sensitive Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

90. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Sensitive Information being placed in the hands of unauthorized third parties and possibly criminals.

91. Plaintiff suffered actual injury from the exposure and theft of her Sensitive Information—which violates her rights to privacy.

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

***Plaintiffs and the Proposed Class Face Significant Risk of Continued Identity Theft***

93. Plaintiffs and members of the proposed Class have suffered injury from the misuse of their Sensitive Information that can be directly traced to Defendant.

94. As a result of Defendant's failure to prevent the Data Breach, Plaintiffs and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their Sensitive Information is used;
b. The diminution in value of their Sensitive Information;
c. The compromise and continuing publication of their Sensitive Information;
d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;
e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;
f. Delay in receipt of tax refund monies;
g. Unauthorized use of stolen Sensitive Information; and

h. The continued risk to their Sensitive Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the Sensitive Information in its possession.

95. Stolen Sensitive Information is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII alone can be worth up to $1,000.00 depending on the type of information obtained.

96. The value of Plaintiffs' and the Class's Sensitive Information on the black market is considerable. Stolen Sensitive Information trades on the black market for years, and criminals frequently post stolen Sensitive Information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

97. It can take victims years to spot identity theft, giving criminals plenty of time to use that information for cash.

98. One such example of criminals using Sensitive Information for profit is the development of "Fullz" packages.

99. Cyber-criminals can cross-reference two sources of Sensitive 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. These dossiers are known as "Fullz" packages.

100. The development of "Fullz" packages means that stolen Sensitive Information from the Data Breach can easily be used to link and identify it to Plaintiffs and the proposed Class' 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 Sensitive Information stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and the Class's stolen Sensitive Information is being misused, and that such misuse is fairly traceable to the Data Breach.

101. Defendant disclosed the Sensitive Information of Plaintiffs and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the Sensitive Information of Plaintiffs and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen Sensitive Information.

102. Defendant's failure to properly notify Plaintiffs and members of the Class of the Data Breach exacerbated Plaintiffs' and the Class's injury by depriving them of the earliest ability to take appropriate measures to protect their Sensitive Information and take other necessary steps to mitigate the harm caused by the Data Breach.

***Defendant failed to adhere to FTC guidelines.***

103. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of Sensitive Information.

104. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the sensitive consumer information that it keeps;

b. properly dispose of Sensitive Information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

105. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

106. The FTC recommends that companies not maintain 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.

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

108. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers, and in this case, its patients' Sensitive Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

***Defendant Violated HIPAA***

109. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information. [9]

110. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and PHI is properly maintained.[10]

111. The Data Breach itself resulted from a combination of inadequacies showing Defendant's failure to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

[9] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, inter alia: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[10] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

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

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

d. Failing to ensure compliance with HIPAA security standards by Defendant in violation of 45 C.F.R. § 164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

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

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

112. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

***Defendant Fails to Comply with Industry Standards***

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

114. Several best practices have been identified that a minimum should be implemented by employers in possession of PII and PHI, 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. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

115. Other best cybersecurity practices that are standard for employers include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

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

117. These foregoing frameworks are existing and applicable industry standards for an employer and company's obligations to provide adequate data security for its employees, or in this case, patients. 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.

## CLASS ACTION ALLEGATIONS

118. Plaintiffs bring this class action under the Florida Rules of Civil Procedure 1.220(a) and (b)(3) individually and on behalf of all members of the following class:

> All individuals residing in the United States whose Sensitive Information was compromised in the Data Breach including all those who received notice of the Data Breach.

119. Excluded from the Class is Defendant, their agents, affiliates, parents, subsidiaries, any entity in which Defendant have a controlling interest, any of Defendant's officers or directors, any successors, and any Judge who adjudicates this case, including their staff and immediate family.

120. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on class-wide bases using the same

evidence as would be used to prove those elements in individual actions asserting the same claims.

a. **Numerosity**. Plaintiffs are representatives of the Class, consisting of at least 225,000 members, far too many to join in a single action;

b. **Ascertainability**. Members of the Class are readily identifiable from information in Defendant's possession, custody, and control;

c. **Typicality**. Plaintiffs' claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiffs will fairly and adequately protect the proposed Class's interests. Their interests do not conflict with the Class's interests, and he has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiffs' and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class. Indeed, it will be necessary to answer the following questions:

    i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiffs' and the Class's Sensitive Information;

    ii. 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;

    iii. Whether Defendant were negligent in maintaining, protecting, and securing Sensitive Information;

iv. Whether Defendant breached contract promises to safeguard Plaintiffs' and the Class's Sensitive Information;

v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendant's Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiffs' and the Class's injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiffs and the Class are entitled to damages, treble damages, or injunctive relief.

121. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

122. Particular issues 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:

i. Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

ii. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

iii. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

iv. Whether an implied contract existed between Defendant on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

v. Whether Defendant breached the implied contract;

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

vii. 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;

viii. Whether Class Members are entitled to actual, consequential, statutory, and/or nominal damages, and injunctive relief as a result of Defendant's wrongful conduct.

123. Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Classes as a whole, making injunctive and declaratory relief appropriate to the Classes as a whole, including:

a. Ordering Defendant to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

b. Ordering that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, Defendant must implement and maintain reasonable security and monitoring measures, including, but not limited to:

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

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

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

v. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;

vi. prohibiting Defendant from maintaining Plaintiffs' and Class Members' Private Information on a cloud-based database until proper safeguards and processes are implemented;

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

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

ix. requiring Defendant to monitor ingress and egress of all network traffic;

x. 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 Private Information, as well as protecting the Private Information of Plaintiffs and Class Members;

xi. 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;

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

xiii. requiring Defendant to meaningfully educate all Class Members about the threats that it faces because of the loss of its confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves; and

xiv. Incidental retrospective relief, including but not limited to restitution.

**COUNT I**
**Negligence**
**(On Behalf of Plaintiffs and the Class)**

124. Plaintiffs reallege all previous paragraphs as if fully set forth below.

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

126. Defendant owed a duty of care to Plaintiffs and Class members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry standards for data security—would compromise their Sensitive Information in a data breach. And here, that foreseeable danger came to pass.

127. Such a duty is codified in Florida law (see e.g., Fla. Stat. §§ 456.057, 501.171).

128. Defendant has full knowledge of the sensitivity of the Sensitive Information and the types of harm that Plaintiffs and the Class could and would suffer if their Sensitive Information was wrongfully disclosed.

129. Defendant owed these duties to Plaintiffs and Class members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiffs and Class members' Sensitive Information.

130. Defendant owed—to Plaintiffs and Class members—at least the following duties to:

a. exercise reasonable care in handling and using the Sensitive Information in its care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. promptly detect attempts at unauthorized access;

d. notify Plaintiffs and Class members within a reasonable timeframe of any breach to the security of their Sensitive Information.

131. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiffs and Class members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiffs and Class members to take appropriate measures to protect their Sensitive Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

132. Defendant also had a duty to exercise appropriate clearinghouse practices to remove Sensitive Information it was no longer required to retain under applicable regulations.

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

134. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class entrusted Defendant with their confidential Sensitive Information, a necessary part of obtaining employment from Defendant.

135. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiffs and Class members' Sensitive Information.

136. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the Sensitive Information entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiffs and the Class members' Sensitive Information.

137. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Sensitive 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 Sensitive Information Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

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

139. 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.

140. Defendant violated its duty under HIPAA by failing to use reasonable measures to protect their PHI and by not complying with applicable regulations detailed *supra*. -

141. The risk that unauthorized persons would attempt to gain access to the Sensitive Information and misuse it was foreseeable. Given that Defendant holds vast amounts of Sensitive Information, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the Sensitive Information —whether by malware or otherwise.

142. Sensitive Information is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Sensitive Information of Plaintiffs and Class members' and the importance of exercising reasonable care in handling it.

143. Defendant improperly and inadequately safeguarded the Sensitive Information of Plaintiffs and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

144. Defendant breached these duties as evidenced by the Data Breach.

145. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs and Class members' Sensitive Information by:

a. disclosing and providing access to this information to third parties and

b. failing to properly supervise both the way the Sensitive Information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

146. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and Sensitive Information of Plaintiffs and Class members which actually and proximately caused the Data Breach and Plaintiffs and Class members' injury.

147. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and Class members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs and Class members' injuries-in-fact.

148. Defendant has admitted that the Sensitive Information of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

149. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and Class members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

150. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiffs and Class members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their Sensitive Information by criminals, improper disclosure of their Sensitive Information, lost benefit of their bargain, lost value of their Sensitive Information, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by

Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

151. Plaintiffs seek actual, consequential, statutory, and/or nominal damages, and injunctive relief as a result of Defendant's wrongful conduct.

**COUNT II**
**Breach of an Implied Contract**
**(On Behalf of Plaintiffs and the Class)**

152. Plaintiffs reallege Paragraphs 1 through 123 above as if fully set forth below.

153. Plaintiffs and the Class delivered their Sensitive Information to Defendant as part of the process of obtaining treatment and services provided by Defendant.

154. Plaintiffs and Class Members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and Class Members if and when their data had been breached and compromised. Each such contractual relationship imposed on Defendant an implied covenant of good faith and fair dealing by which Defendant was required to perform its obligations and manage Plaintiffs' and Class Members' data in a manner which comported with the reasonable expectations of privacy and protection attendant to entrusting such data to Defendant.

155. In providing their Sensitive Information, Plaintiffs and Class Members entered into an implied contract with Defendant whereby Defendant, in receiving such data, became obligated to reasonably safeguard Plaintiffs' and the other Class Members' Sensitive Information.

156. In delivering their Sensitive Information to Defendant, Plaintiffs and Class Members intended and understood that Defendant would adequately safeguard that data.

157. Plaintiffs and the Class Members would not have entrusted their Sensitive Information to Defendant in the absence of such an implied contract.

158. Defendant accepted possession of Plaintiffs' and Class Members' Sensitive Information.

159. Had Defendant disclosed to Plaintiffs and Class Members that Defendant did not have adequate computer systems and security practices to secure patients' Sensitive Information, Plaintiffs and members of the Class would not have provided their Sensitive Information to Defendant.

160. Defendant recognized that patients' Sensitive Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiffs and Class Members.

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

162. Defendant breached the implied contract with Plaintiffs and Class Members by failing to take reasonable measures to safeguard its data.

163. Defendant breached the implied contract with Plaintiffs and Class Members by failing to promptly notify them of the access to and exfiltration of their Sensitive Information.

164. As a direct and proximate result of the breach of the contractual duties, Plaintiffs and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiffs and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiffs' and Class Members' Sensitive Information; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and

prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their Sensitive Information; (g) the diminution in the value of the services bargained for as Plaintiffs and Class Members were deprived of the data protection and security that Defendant promised when Plaintiffs and the proposed class entrusted Defendant with their Sensitive Information; and (h) the continued and substantial risk to Plaintiffs' and Class Members' Sensitive Information, which remains in the Defendant's possession with inadequate measures to protect Plaintiffs' and Class Members' Sensitive Information.

165. Plaintiffs seek actual, consequential, statutory, and/or nominal damages, and injunctive relief as a result of Defendant's wrongful conduct.

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

166. Plaintiffs reallege Paragraphs 1 through 123 above as if fully set forth below.

167. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

168. Plaintiffs and members of the Class conferred a benefit upon Defendant in providing Sensitive Information to Defendant.

169. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and the Class. Defendant also benefited from the receipt of Plaintiffs' and the Class's Sensitive Information, as this was used to facilitate the treatment, services, and goods it sold to Plaintiffs and the Class.

170. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs and the Class's Sensitive Information because

Defendant failed to adequately protect their Sensitive Information. Plaintiffs and the proposed Class would not have provided their Sensitive Information to Defendant had they known Defendant would not adequately protect their Sensitive Information.

171. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and members of the Class all unlawful or inequitable proceeds received by them because of their misconduct and Data Breach.

**COUNT IV**
**Invasion of Privacy—Intrusion Into Seclusion**
**(On Behalf of Plaintiffs and the Class)**

172. Plaintiffs reallege Paragraphs 1 through 123 above as if fully set forth below.

173. Plaintiffs and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential Sensitive Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

174. Defendant owed a duty to its current and former patients, including Plaintiffs and the Class, to keep this information confidential.

175. The unauthorized acquisition (i.e., theft) by a third party of Plaintiffs and Class members' Sensitive Information is highly offensive to a reasonable person.

176. The intrusion was into a place or thing which was private and entitled to be private. Plaintiffs and the Class disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

177. The Data Breach constitutes an intentional interference with Plaintiffs' and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

178. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

179. Defendant acted with a knowing state of mind when it failed to notify Plaintiffs and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

180. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

181. As a proximate result of Defendant's acts and omissions, the private and Sensitive Information of Plaintiffs and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages (as detailed *supra*).

182. And, on information and belief, Plaintiffs' Sensitive Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

183. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their Sensitive Information are still maintained by Defendant with their inadequate cybersecurity system and policies.

184. Plaintiffs and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment

for monetary damages will not end Defendant's inability to safeguard the Sensitive Information of Plaintiffs and the Class.

185. In addition to injunctive relief, Plaintiffs, on behalf of themselves and the other Class members, also seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

**COUNT V**
**Violation of Florida Deceptive and Unfair Trade Practices Act**
**Fla. Stat. §§ 501.201, *et seq*.**
**(On Behalf of Plaintiffs and the Class)**

186. Plaintiffs reallege Paragraphs 1 through 123 above as if fully set forth below.

187. This cause of action is brought under the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA").

188. The purpose of FDUTPA is to "protect the consuming public and legitimate business enterprises from those who engage in unfair methods of competition, or unconscionable, deceptive, or unfair acts or practices in the conduct of any trade or commerce." Fla. Stat. § 501.202(2).

189. Another purpose of FDUTPA is to construe consumer protection as "consistent with established policies of federal law relating to consumer protection." Fla. Stat. § 501.202(3).

190. Plaintiffs and Class members all constitute "[c]onsumers" under FDUTPA because they are all "individual[s]." Fla. Stat. § 501.203.

191. Plaintiffs and Class members each constitute an "[i]nterested party or person" under FDUTPA because they are all "affected by a violation" of FDUTPA. Fla. Stat. § 501.203.

192. FDUTPA applies to Defendant because Defendant engages in "[t]rade or commerce" as defined as "advertising, soliciting, providing, offering, or distributing, whether by sale, rental, or otherwise, of any good or service, or any property, whether tangible or intangible, or any other article, commodity, or thing of value, wherever situated." Fla. Stat. § 501.203.

193. FDUTPA declares as unlawful "unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce." Fla. Stat. § 501.204(1).

194. FDUTPA provides that "due consideration be given to the interpretations of the Federal Trade Commission and the federal courts relating to Section 5(a)(1) of the Trade Commission Act." Fla. Stat. § 501.204(2).

195. Relevant here, is that "[v]iolation[s]" of FDUTPA is broadly defined to include violations of:

a. "Any rules promulgated pursuant to the Federal Trade Commission Act, 15 U.S.C. ss. 41 *et seq*." Fla. Stat. § 501.203.

b. "The standards of unfairness and deception set forth and interpreted by the Federal Trade Commission or the federal courts." Fla. Stat. § 501.203.

c. "Any law, statute, rule, regulation, or ordinance which proscribes unfair methods of competition, or unfair, deceptive, or unconscionable acts or practices." Fla. Stat. § 501.203.

196. Under FCRA, HIPAA (42 U.S.C. § 1302d *et seq*.), the FTCA, and Florida law (Fla. Stat. § 456.057 and § 501.171), Defendant was required by law to maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiffs'

and Class members' Sensitive Information. Defendant was also under an obligation expressly under Florida law, where Defendant is headquartered and managed, to adequately protect Plaintiffs' and Class members' Sensitive Information.

197. Moreover, FDUTPA requires that Defendant (1) take reasonable measures to protect and secure data in electronic form containing Sensitive Information; (2) take reasonable measures to dispose of or destroy Sensitive Information; and (3) provide notice to consumers and consumer reporting agencies subject to the FCRA when a data security incident occurs that compromises Sensitive Information. Fla. Stat. §§ 501.171.

198. Defendant violated FDUTPA by, *inter alia*:

a. failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class members' Sensitive Information which was a direct and proximate cause of the Data Breach;

b. failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' Sensitive Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq*., which was a direct and proximate cause of the Data Breach;

d. omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class members' Sensitive Information; and

e. omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' Sensitive Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq*.

199. Defendant's omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of their Sensitive Information.

200. Defendant intended to mislead Plaintiffs and Class members and induce them to rely on its omissions.

201. Had Defendant disclosed to Plaintiffs and Class members that its data systems were not secure—and thus vulnerable to attack—Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Defendant accepted the Sensitive Information that Plaintiffs and Class members (or their third-party agents) entrusted to it while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiffs and Class members acted reasonably in relying on Defendant's omissions, the truth of which they could not have discovered through reasonable investigation.

202. Defendant acted intentionally, knowingly, maliciously, and recklessly disregarded Plaintiffs' and Class members' rights.

203. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiffs and Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including

from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Sensitive Information.

204. Plaintiffs and Class members seek declaratory judgement that Defendant's practices were unreasonable and inadequate and thus caused the Data Breach.

205. Plaintiffs and Class members seek injunctive relief enjoining the wrongful acts described *supra* and requiring Defendant to use and maintain proper standards for data security including, *inter alia*, proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing. Fla. Stat. § 501.211(1).

206. Plaintiffs and Class members seek all monetary and non-monetary relief allowed by law. Plaintiffs seek actual damages, attorneys' fees, and costs under Fla. Stat. §§ 501.2105, 501.211(2).

## PRAYER FOR RELIEF

Plaintiffs and the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiffs and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen Sensitive Information;

E. Awarding Plaintiffs and the Class damages that include applicable compensatory, exemplary, nominal, punitive, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

Dated: October 24, 2024

*/s/ Jeff Ostrow*

Jeff Ostrow (FL Bar No. 121452)
**KOPELOWITZ OSTROW P.A.**
One West Las Olas Boulevard, Suite 500
Fort Lauderdale, Florida 33301
Ph: 954-525-4100
ostrow@kolawyers.com

Samuel J. Strauss (*pro hac vice* pending)
**STRAUSS BORRELLI PLLC**
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
(872) 263-1100
(872) 263-1109 (facsimile)
sam@straussborrelli.com

Manuel S. Hiraldo, Esq.
**HIRALDO P.A.**
Florida Bar No. 030380

401 E. Las Olas Boulevard
Suite 1400
Ft. Lauderdale, Florida 33301
Email: mhiraldo@hiraldolaw.com
Telephone: 954.400.4713

John A. Yanchunis
Florida Bar #: 324681
JYanchunis@forthepeople.com
**MORGAN & MORGAN**
**COMPLEX LITIGATION GROUP**
201 North Franklin Street 7th Floor
Tampa, FL 33602
T: (813) 223-5505
F: (813) 223-5402

*Plaintiffs' Interim Class Counsel*

**CERTIFICATE OF SERVICE**

I hereby certify that on October 24, 2024, a copy of the foregoing pleading was filed electronically with the Clerk of Court to be served by operation of the court's electronic filing system to all counsel of record.

/s/ *Jeff Ostrow*
Jeff Ostrow

# EXHIBIT A

Return Mail Processing
P.O. Box 3826
Suwanee, GA 30024

<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<Date>

**NOTICE OF DATA <<SECURITY EVENT/BREACH>>**

Dear <<Full Name>>:

South Florida Behavioral Health Network ("SFBHN") d/b/a Thriving Mind South Florida is writing to inform you of a data privacy incident that impacts some of your information. SFBHN provides management services to a network of providers offering care to individuals with substance abuse and mental health disorders in Miami-Dade and Monroe counties. Although we have no indication of actual fraud or misuse of your information as a result of the incident, we are providing you with information about the incident, our response to it, and resources available to you to help protect your information, should you feel it appropriate to do so.

**What Happened?** On August 3, 2023, SFBHN became aware of suspicious activity on certain computer systems in our environment. We immediately took steps to secure our environment and launched an investigation with third-party specialists to determine the full nature and scope of the activity. The investigation determined that an unauthorized actor gained access to our servers between August 1 and August 3, 2023, and during this time certain internal files were obtained without authorization. In response, we undertook an extensive review of the files at issue through a third-party vendor, which was completed on March 25, 2024. We have been working since this time to review and verify the information at issue and provide an accurate notice to those who were affected.

**What Information Was Involved?** The information contained in the affected files includes your name and <<data elements>>. To date, we are unaware of any actual misuse of this information as a result of the event.

**What We Are Doing**. The privacy and security of information in our possession is one of our highest priorities. We conducted a thorough investigation to determine the scope of the incident and worked quickly to secure our systems. We also notified federal law enforcement as well as applicable state and federal regulators. To help prevent similar future incidents, we are further enhancing our network security through the use of additional security tools and protocols.

While we have no indication of your information being misused in connection with this incident, as an extra precaution, we are offering you access to <<12/24 Months>> of complimentary credit monitoring and identity restoration services through CyEx.

**What You Can Do.** We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits statements, and monitoring your free credit reports for suspicious activity and to detect errors. You may also review the information contained in the enclosed *Steps You Can Take to Help Protect Your Information*. There you will also find more information on the credit monitoring and identity restoration services we are making available to you. While SFBHN will cover the cost of these services, you will need to follow the enrollment instructions to enroll yourself in the services. Enrollment instructions are enclosed with this letter.

**For More Information.** If you have additional questions, please call us at 1-888-498-4056. This toll-free line is available Monday – Friday from 9:00 am to 9:00 pm Eastern Time (excluding major U.S. Holidays). You may also write to SFBHN at 7205 NW 19th St. Ste 200, Miami, Florida, 33126-1228.

We apologize for any inconvenience to you and remain dedicated to protecting the information in our care.

Sincerely,

**South Florida Behavioral Health Network ("SFBHN") d/b/a Thriving Mind South Florida**

## STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

**Enroll in Credit and Identity Monitoring**

# Identity Defense Complete

### Enrollment Instructions

1. Visit: **app.identitydefense.com/enrollment/activate/sfbh**
2. Enter your unique Activation Code: **<<Activation Code>>**
3. Click 'Redeem Code'
4. Follow the prompts to create your account

**The deadline to enroll is <<Enrollment Deadline>>.** After <<Enrollment Deadline>>, the enrollment process will close, and your Identity Defense code will no longer be active. **If you do not enroll by <<Enrollment Deadline>>, you will not be able to take advantage of Identity Defense, so please enroll before the deadline.**

### Key Features

- 1-Bureau Credit Monitoring
- Monthly Credit Score and Tracker (VantageScore 3.0)
- Real-Time Authentication Alerts
- High-Risk Transaction Monitoring
- Address Change Monitoring
- Dark Web Monitoring
- Wallet Protection
- Security Freeze Assist
- $1 Million Identity Theft Insurance**

If you need assistance with the enrollment process or have questions regarding Identity Defense, please call Identity Defense directly at **1-866-622-9303.**

**Monitor Your Accounts**

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you may need to provide the following information, depending on whether the request is made online, by phone, or by mail:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

| **Equifax** | **Experian** | **TransUnion** |
|---|---|---|
| https://www.equifax.com/personal/credit-report-services/ | https://www.experian.com/help/ | https://www.transunion.com/credit-help |
| 1-888-298-0045 | 1-888-397-3742 | 1-800-916-8800 |
| Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069 | Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013 | TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016 |
| Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788 | Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013 | TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094 |

**Additional Information**

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state attorney general. This notice has not been delayed by law enforcement.

*For District of Columbia residents*, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 1-202-727-3400; and oag@dc.gov.

*For Maryland residents*, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

*For New Mexico residents*, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

*For New York residents,* the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

*For North Carolina residents*, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

*For Rhode Island residents*, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this event. There are approximately <<RI Count>> Rhode Island residents impacted by this event.

# ClassAction.org



---