IN THE CIRCUIT COURT OF THE THIRTEENTH JUDICIAL CIRCUIT IN AND FOR HILLSBOROUGH COUNTY, FLORIDA

JEREMY REARDON, LINDA POTTER, and FRANKIE SOLOMON, individually and on behalf of all similarly situated persons, Plaintiffs, v. SUNCOAST SKIN SOLUTIONS, INC., Defendant.	**Civil Action No.: 23-CA-000317** PROPOSED CLASS ACTION JURY TRIAL DEMANDED

AMENDED CLASS ACTION COMPLAINT

Plaintiffs, Jeremy Reardon, Linda Potter, and Frankie Solomon, (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated, upon personal knowledge of the facts pertaining to themselves and on information and belief as to all other matters, by and through counsel, hereby bring this Amended Class Action Complaint against Defendant, Suncoast Skin Solutions, Inc ("Suncoast").

NATURE OF THE ACTION

1. In July 2021, Suncoast, a dermatology clinic system with 19 locations in Florida, lost control over its patients' highly sensitive personal information in a data breach by cybercriminals ("Data Breach").

2. The Data Breach exposed the "protected health information" ("PHI") belonging to over 70,000 patients, including records on their cancer treatments, surgeries, and cosmetic procedures. That exposure disturbs patients, as they no longer control their highly sensitive medical records, cannot stop others from viewing it, and cannot prevent criminals from misusing it.

3. What's more, the Data Breach exposed patients' "personally identifiable information" ("PII"), exposing them to an increased lifelong risk for identity theft and fraud. Indeed, the Data Breach included information patients cannot change, like Social Security numbers and birth dates.

4. Worse, Suncoast exacerbated the harm its patients are suffering by failing to notify them about the Data Breach for *1.5 years*, meaning its patients had no reason to guard themselves against identity theft and fraud while criminals had their information and could misuse it.

5. Suncoast's Data Breach should not have happened because it was preventable.

6. As a medical provider, Suncoast knows it has duties to safeguard its patients' information, affirming that "[d]ata privacy and security is among Suncoast's highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information in our care."

7. Its patients, like Ms. Potter and Mr. Solomon, relied on Suncoast to fulfill its duties when they agreed to treat with Suncoast, and they would not have treated if Suncoast had not promised to protect their PHI and PII (together "Personal Information").

8. For those patients whose Personal Information was acquired by Suncoast through mergers and acquisitions with other physicians' offices, like that of Mr. Reardon, it is equally true that those individuals would not have consented to their Personal Information being transferred to Suncoast if they knew that Suncoast would not protect their Personal Information.

9. Even so, Suncoast never implemented the security safeguards that it was obligated use to protect that data.

10. Indeed, on information and belief, Suncoast failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to

lose control over the access to patient Personal Information. Suncoast's negligence is evidenced by its failure to prevent, detect, or stop the Data Breach before criminals gained access to Suncoast's systems and stole the information belonging to over 70,000 patients.

11. And Suncoast exacerbated the harm its patients are suffering because it delayed notifying them about the Data Breach for over 18 months, depriving them of the earliest opportunity to mitigate the harm the Data Breach causes.

12. Suncoast's misconduct violates state and federal law and industry standard data security policies.

13. On information and belief, Plaintiffs are current and former Suncoast patients who disclosed their Personal Information to Suncoast (or physicians whose practices that Suncoast acquired as a successor in interest) to receive medical services.

14. Plaintiffs are also Data Breach victims, having received Suncoast's Data Breach notice in December 2022.

15. Since Suncoast's Data Breach, Plaintiffs have suffered identity theft and fraud, harm they had no ability to mitigate due to Suncoast's delayed notice.

16. Plaintiffs bring this Class Action on behalf of themselves and all others harmed by Suncoast's misconduct.

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 in excess of $50,000.00, exclusive of interest and attorneys' fees.

18. Venue is proper in Hillsborough County pursuant to Florida Stat. § 47.011 and § 47.051 because Suncoast is headquartered and does business in this county, the cause of action

accrued in this county, and Suncoast has an office for the transaction of its customary business in this county.

19. The Court has personal jurisdiction over Suncoast because under Florida Stat. § 48.193, Suncoast 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 Suncoast engaged in significant business activity within Florida.

FACTUAL BACKGROUND

A. Suncoast Collects and Promises to Protect Patients' Personal Information

20. Suncoast is a system of dermatology clinics with 19 locations around Florida.

21. Holding itself out as "Florida's Most Trusted Dermatology Group," it offers patients services treating skin cancer, medical dermatology, and cosmetic dermatology.

22. To operate its business, Suncoast must create, collect, and store patients' Personal Information.

23. As a result, Suncoast requires its patients to disclose their Personal Information to receive Suncoast's services, including their names, Social Security numbers, dates of birth, clinical information, doctor's notes, and "other limited treatment information."

24. In so doing, Suncoast promises those patients it will protect their information under state and federal law and its internal policies.

25. In fact, Suncoast assures patients it is "dedicated to ensuring the privacy and security of all information in [its] control" and that "[d]ata privacy and security is among Suncoast's highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information in our care." In other words, Suncoast recognizes

it has duties to safeguard patients' Personal Information. *See* Suncoast's Data Breach Notice ("Notice," previously attached as **Exhibit A** to the initial Complaint).

26. But Suncoast never implemented the security safeguards necessary to fulfill those duties, failing to adequately train its employees on data security, develop policies to prevent breaches, enforce those policies, follow industry standard guidelines on cybersecurity, and timely respond to data breaches and inform patients as required by law.

27. As a result, Suncoast left patients' Personal Information an unguarded target for theft and misuse.

B. Suncoast Acquired Patients' Personal Information Through Mergers and Acquisitions

28. In addition to requiring its patients to disclose their Personal Information to receive Suncoast's services, on information and belief Suncoast has acquired other physicians' practices through mergers, acquisitions, and other like means and thereby acquired other patients' Personal Information.

29. Although those patients may not have treated with Suncoast after their original physicians sold or otherwise transitioned their practices to Suncoast, Suncoast owed the same duties to those patients as it did any current patient: to protect their information under state and federal law and its internal policies.

C. Suncoast Violates Its Duties

30. In July 2021, Suncoast discovered "unusual activity on its network."

31. That "activity" was a data breach by cybercriminals, who bypassed Suncoast's lax security and infiltrated its systems.

32. Once inside, hackers could access patients' Personal Information, including their names, addresses, dates of birth, Social Security numbers, and medical records.

33. On information and belief, the Data Breach was a "ransomware" attack, meaning criminals blocked Suncoast's access to patient data and held it ransom.

34. In response, Suncoast claims it "disconnected all access to the network and promptly engaged a specialized third-party cybersecurity firm to assist with securing the environment, as well as, to conduct a comprehensive forensic investigation to determine the nature and scope of the incident"—an investigation that would drag on for four months.

35. During that time, Suncoast did not warn patients that it lost control over their data, meaning they had no reason to guard themselves against identity theft and fraud. This also meant that patients continued to treat with Suncoast, providing their Personal Information to an unsecure healthcare provider and Suncoast continuing to collect revenue associated with ongoing treatment.

36. In November 2021, Suncoast completed its investigation and determined that the Data Breach resulted in the exposure of patients' Personal Information to unauthorized third parties—namely, the hackers who gained entry to Suncoast's systems. Still, it did not notify its patients about the Data Breach, keeping them in the dark and depriving them of the earliest opportunity to prevent and mitigate identity theft and fraud.

37. For the next year, Suncoast engaged in a "data mining" process to determine which patients its Data Breach affected, without explaining why the process took 12 months.

38. In December 2022, Suncoast finally completed its process and notified patients about the Data Breach. *See* **Exhibit A**.

39. In its Notice, Suncoast recognized the threat its Data Breach posed to its patients. Indeed, it advised patients to "remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all

major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file."

40. In other words, Suncoast encouraged its patients to spend time and resources mitigating the harm resulting from the Data Breach—after Suncoast inexplicably delayed notifying those patients in a timely fashion.

41. Suncoast foresaw the harm that would result from the Data Breach; indeed as Plaintiffs have suffered harm, including identity theft and fraud, following Suncoast's Data Breach.

D. Plaintiffs' Experiences

Plaintiff Reardon's Experience

42. On information and belief, Mr. Reardon treated with a physician who subsequently sold or transitioned that practice to Suncoast. That sale or transition resulted in Mr. Reardon's Personal Information being transferred from that former practice to the custody and control of Suncoast.

43. Mr. Reardon is also a victim of the Data Breach, having received Suncoast's Notice in December 2022.

44. Mr. Reardon provided his Personal Information to his physician and trusted that his physician would use reasonable measures to protect it. On information and belief, Mr. Reardon's Personal Information was subsequently provided to Suncoast through a sale or transition of his former physician's practice, and Mr. Reardon expected that information would be protected according to state and federal law and any applicable internal policies at the new company—here, Suncoast.

45. Since the Data Breach, Mr. Reardon has suffered repeated identity theft and fraud.

Mr. Reardon received correspondence from Bank of America asking him to verify his email address, followed by an email explaining that "his" credit card application was received. But Mr. Reardon never applied for that card and never authorized anyone else to apply for him. Despite trying to cancel the card, he has received notifications that "his" account was enrolled in online and mobile banking. Enrollment for a new credit card account would require Mr. Reardon's Social Security Number and other PII that was compromised in the Data Breach.

46. In addition, since the Data Breach occurred, Mr. Reardon has received security alerts that his Social Security number was found on the dark web.

47. To deal with this fraud and identity theft, Mr. Reardon has devoted at least 25 hours to remediating it and mitigating the potential for it to happen again.

48. Indeed, Mr. Reardon has and will spend considerable time and effort monitoring his accounts to protect himself from identity theft. Mr. Reardon fears for his personal financial security and uncertainty over what Personal Information was exposed in the Data Breach.

49. Mr. Reardon has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. The fear stems from the fact that his highly sensitive Personal Information is in criminal hands, who have already shown they will misuse his information. These emotional harms go 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.

50. Mr. Reardon 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, Mr. Reardon will continue to be at present, imminent, and continued increased risk of identity theft and fraud for years to come.

51. Mr. Reardon does not recall ever learning that his information was compromised in a data breach incident, other than the Data Breach at issue in this case.

52. Mr. Reardon suffers a present injury from the increased risk of fraud, identity theft, and misuse resulting from his Personal Information being placed in the hands of criminals. Mr. Reardon has a continuing interest in ensuring that his Personal Information, which is the type that cannot be changed and upon information and belief remains in Suncoast's possession, is protected and safeguarded from future breaches.

53. Suncoast has not represented the business practices changes that have been implemented to prevent against further data breaches—even at a high level that would not jeopardize its security infrastructure.

Plaintiff Potter's Experience

54. On information and belief, Ms. Potter treated with Suncoast in the past, but terminated that relationship. Ms. Potter was referred to Suncoast by her primary care physician.

55. Ms. Potter is also a Data Breach victim, having received Suncoast's Notice in December 2022.

56. As a condition to receiving Suncoast's services, Suncoast required Ms. Potter to disclose her Personal Information.

57. Ms. Potter provided her Personal Information to Suncoast and trusted that the company would use reasonable measures to protect it according to Suncoast's internal policies and state and federal law.

58. Since Ms. Potter terminated her relationship with Suncoast, Ms. Potter was surprised to learn that Suncoast kept her Personal Information in its systems—and she learned this through her receipt of Suncoast's Notice in December 2022.

59. Ms. Potter has and will spend considerable time and effort monitoring her accounts

to protect herself from identity theft. Ms. Potter fears for her personal financial security and uncertainty over what PII was exposed in the Data Breach.

60. Ms. Potter has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. The fear stems from the fact that her highly sensitive Personal Information is in criminal hands, who have the ability to misuse her information. These emotional harms go 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.

61. Ms. Potter does not recall ever learning that her information was compromised in a data breach incident, other than the Data Breach at issue in this case.

62. Ms. Potter suffers a present injury from the increased risk of fraud, identity theft, and misuse resulting from her Personal Information being placed in the hands of criminals. Ms. Potter has a continuing interest in ensuring that her Personal Information, which is the type that cannot be changed and upon information and belief remains in Suncoast's possession, is protected and safeguarded from future breaches.

63. Suncoast has not represented the business practices changes that have been implemented to prevent against further data breaches—even at a high level that would not jeopardize its security infrastructure.

Plaintiff Solomon's Experience

64. On information and belief, Mr. Solomon is a current Suncoast patient, referred to Suncoast by his primary care physician.

65. Mr. Solomon is also a Data Breach victim, having received Suncoast's Notice in December 2022.

66. As a condition to receiving Suncoast's services, Suncoast required Mr. Solomon to disclose his Personal Information.

67. Mr. Solomon provided his Personal Information to Suncoast and trusted that the company would use reasonable measures to protect it according to Suncoast's internal policies and state and federal law.

68. Indeed, Mr. Solomon has and will spend considerable time and effort monitoring his accounts to protect himself from identity theft. Mr. Solomon fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach.

69. Mr. Solomon has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. The fear stems from the fact that his highly sensitive Personal Information is in criminal hands, who have the ability to misuse his information. These emotional harms go 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.

70. Mr. Solomon does not recall ever learning that his information was compromised in a data breach incident, other than the Data Breach at issue in this case.

71. Mr. Solomon suffers a present injury from the increased risk of fraud, identity theft, and misuse resulting from his Personal Information being placed in the hands of criminals. Mr. Solomon has a continuing interest in ensuring that his Personal Information, which is the type that cannot be changed and upon information and belief remains in Suncoast's possession, is protected and safeguarded from future breaches.

72. Suncoast has not represented the business practices changes that have been implemented to prevent against further data breaches—even at a high level that would not jeopardize its security infrastructure.

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

73. Plaintiffs and members of the proposed Class have suffered injury from the misuse of their Personal Information that can be directly traced to Suncoast.

74. As a result of Suncoast'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 Personal Information is used;

b. The compromise and continuing publication of their Personal Information;

c. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

d. 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;

e. Delay in receipt of tax refund monies;

f. Unauthorized use of stolen Personal Information; and

g. The continued increased risk to their Personal Information, which remains in the possession of Suncoast and is subject to further breaches so long as Suncoast fails to undertake the appropriate measures to protect the Personal Information in their possession.

75. Stolen Personal Information are one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen Personal Information can be worth up to $1,000.00 depending on the type of information obtained. Thus, criminals willingly pay money for access to Personal Information, which enables those criminals to commit fraud and identity theft to the detriment of patients and consumers, including Plaintiffs and members of the Class.

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

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

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

79. Cyber-criminals can cross-reference two sources of Personal 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.

80. The development of "Fullz" packages means that stolen Personal Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and the proposed Class's phone numbers, email addresses, and other 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 Personal 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 other members of the proposed Class's stolen Personal Information are being misused, and that such misuse is fairly traceable to the Data Breach.

81. Suncoast disclosed the Personal Information of Plaintiffs and members of the

proposed Class to unauthorized third parties to use in the conduct of criminal activity. Specifically, Suncoast exposed the Personal Information of the Plaintiffs and members of the proposed 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 Personal Information.

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

83. Had Suncoast timely and properly notified Plaintiffs and members of the proposed Class of the Data Breach, Plaintiffs and members of the proposed Class could have taken proactive, rather than reactive, mitigating measures. Plaintiffs, had they received timely notice, could have placed a freeze on their credit, which should have prevented the criminal activity (*e.g.*, for Mr. Reardon the new credit card being opened) from occurring.

F. Suncoast failed to adhere to FTC guidelines.

84. 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 Suncoast, should employ to protect against the unlawful exposure of Personal Information.

85. 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 personal customer information that they keep;

b. properly dispose of personal 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.

86. 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.

87. 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.

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

89. Suncoast's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' (*i.e.*, consumers') Personal Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

G. Suncoast Failed to Adhere to HIPAA

90. 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.[1]

91. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PHI is properly maintained.[2]

92. The Data Breach itself resulted from a combination of inadequacies showing Suncoast failed to comply with safeguards mandated by HIPAA. Suncoast'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);

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 Suncoast workforce 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

[1] 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.

[2] *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).

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).

CLASS REPRESENTATION ALLEGATIONS

93. Plaintiffs bring this suit on behalf of themselves and a class of similarly situated individuals under Florida Rule of Civil Procedure 1.220 on behalf of a class preliminarily defined as:

> All persons impacted by the Data Breach, including all who were sent a notice of the Data Breach. Excluded from the class are all employees, officers, and directors of Defendant, as well as any judges presiding over this matter and court personal assigned to this case.

94. **Numerosity**: The Class Members are so numerous that joinder of all members is impracticable. The exact number and identities of Class Members are unknown at this time, but are reported to be at least the 70,000 to whom Suncoast sent the Notice. The identities of Class Members are ascertainable through Suncoast's records, Class Members' records, publication notice, self-identification, and other means.

95. **Commonality:** Common questions of law and fact exist as to all Class Members. These common questions of law or fact predominate over any questions affecting only individual members of the Class. Common questions include, but are not limited to, the following:

(a) Whether Suncoast violated state and federal laws by failing to properly store, secure, and dispose of Plaintiffs' and Class Members' Personal Information;

(b) Whether Suncoast failed to employ reasonable and adequate data and cybersecurity measures in compliance with applicable state and federal regulations;

(c) Whether Suncoast acted willfully, recklessly, or negligently with regard to securing Plaintiffs' and Class Members' Personal Information;

(d) How the Data Breach occurred;

(e) Whether Suncoast failed to timely notify Plaintiffs and Class Members of the Data Breach;

(f) Whether Plaintiffs and Class Members are entitled to restitution, damages, compensation, or other monetary relief; and

(g) Whether Plaintiffs and Class Members are entitled to injunctive and declaratory relief necessary to secure their Personal Information from further intrusion, exposure, and misuse.

96. Common sources of evidence may also be used to demonstrate Suncoast's unlawful conduct on a class-wide basis, including, but not limited to, documents and testimony about its data and cybersecurity measures (or lack thereof); testing and other methods that can prove Suncoast's data and cybersecurity systems have been or remain inadequate; documents and

testimony about the source, cause, and extent of the Data Breach; and documents and testimony about any remedial efforts undertaken as a result of the Data Breach.

97. **Typicality:** Plaintiffs' claims are typical of the claims of the respective Class they seek to represent, in that the named Plaintiffs and all members of the proposed Class have suffered similar injuries as a result of the same practices alleged herein. Plaintiffs have no interests adverse to the interests of the other members of the Class.

98. **Adequacy:** Plaintiffs will fairly and adequately protect the interests of the Class and have retained attorneys well experienced in class actions and complex litigation as their counsel, including cases alleging consumer protection and data privacy claims arising from medical data breaches.

99. The Class also satisfies the criteria for certification under Florida Rule of Civil Procedure 1.220(b). Among other things, Plaintiffs aver that the prosecution of separate actions by the individual members of the proposed Class would create a risk of inconsistent or varying adjudication which would establish incompatible standards of conduct for Suncoast; that the prosecution of separate actions by individual class members would create a risk of adjudications with respect to them which would, as a practical matter, be dispositive of the interests of other class members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; that Suncoast has acted or refused to act on grounds that apply generally to the proposed Class, thereby making final injunctive relief or declaratory relief described herein appropriate with respect to the proposed Class as a whole; that questions of law or fact common to the Class predominate over any questions affecting only individual members and that class action treatment is superior to other available methods for the fair and efficient adjudication of the controversy which is the subject of this action. Plaintiffs further state that the interests of judicial

economy will be served by concentrating litigation concerning these claims in this Court, and that the management of the Class will not be difficult.

100. Plaintiffs and other members of the Class have suffered injury, harm, and damages as a result of Suncoast's unlawful and wrongful conduct. Absent a class action, Suncoast will continue to maintain Class Members' Personal Information that could be subject to future breaches due to lax or non-existent cybersecurity measures, and such unlawful and improper conduct should not go unchecked nor remedied. Absent a class action, the members of the Class will not be able to effectively litigate these claims and will suffer further harm and losses, as Suncoast will be allowed to continue such conduct with impunity and benefit from its unlawful conduct.

CLAIMS FOR RELIEF

COUNT I
Violation of Florida Deceptive and Unfair Trade Practices Act,
Fla. Stat. §§ 501.201, et seq.
On behalf of Plaintiffs and the Class

101. Plaintiffs reallege paragraphs 1 through 100 above as if fully set forth herein. Plaintiffs bring this claim on behalf of the Class set forth above.

102. This cause of action is brought pursuant to the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"). Fla. Stat. §§ 501.201, et seq. The express purpose of FDUPTA is to "protect the consuming public . . . 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).

103. Suncoast's sale of goods and provision of medical services for monetary compensation at issue in this cause are "consumer transaction[s]" within the scope of FDUTPA. Fla. Stat. §§ 501.201-501.213. Plaintiffs are "consumer[s]" as defined by FDUTPA. Fla. Stat. § 501.203. Suncoast is engaged in trade or commerce within the meaning of FDUTPA.

104. 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).

105. FDUPTA 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). Suncoast's unfair and deceptive practices are likely to mislead—and have misled—the consumer acting reasonably under the circumstances. Fla. Stat. § 500.04; 21 U.S.C. § 343. As set forth above, Suncoast's Data Breach was a result of its substandard (if not wholly inadequate) data and cybersecurity practices in violation of the state and federal requirements as set forth above.

106. Pursuant to the FCRA, HIPAA (42 U.S.C. § 1302d et seq.), the FTCA, and Florida law (Fla. Stat. § 456.057 and § 501.171), Suncoast was required by law to maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiffs' and Class Members' Personal Information. Suncoast was also under an obligation expressly under Florida law, where Suncoast is headquartered and managed, to adequately protect Plaintiffs' and Class Members' Personal Information. Among other things, Florida requires Suncoast to (1) take reasonable measures to protect and secure data in electronic form containing PII; (2) take reasonable measures to dispose of or destroy PII; and (3) provide notice to consumers and consumer reporting agencies subject to the FCRA when a data security incident occurs that compromises PII. Fla. Stat. §§ 501.171.

107. Suncoast has violated FDUPTA by engaging in the unfair and deceptive practices described above, which offend public policies and are immoral, unethical, unscrupulous and substantially injurious to consumers. At all times material herein, Suncoast has failed to maintain

adequate and reasonable data and cybersecurity protocols for Plaintiffs' and Class Members' Personal Information in violation of state and federal laws and its own privacy practices and policies. Suncoast has also failed to take reasonable measures to destroy or dispose of Personal Information and timely notify its patients of the Data Breach in violation of Florida law.

108. Plaintiffs have standing to pursue this claim because they have been injured by virtue of suffering a loss of privacy, money and/or property as a result of the wrongful conduct alleged herein. Plaintiffs would not have purchased Suncoast's goods and services (or paid as much) had they known the truth about Suncoast's substandard and shoddy data and cybersecurity measures. Moreover, Suncoast will continue to maintain Plaintiffs' and Class Members' Personal Information for the indefinite future, giving them a strong interest in ensuring such data is protected with state of the art, industry standards to prevent future data breaches. This is as true for current patients (*e.g.*, Mr. Solomon), former patients (*e.g.*, Ms. Potter), and those whose Personal Information were obtained from other physicians (*e.g.*, Mr. Reardon). As a direct result of Suncoast's actions and omissions of material facts, Plaintiffs and Class Members did not obtain the value of the goods and services for which they paid; were induced to pay for (or pay more for) medical goods and services that they otherwise would not have; and lost their ability to make informed and reasoned decisions about their medical treatment.

109. The damages suffered by Plaintiffs and Class Members were directly and proximately caused by the deceptive, misleading and unfair practices of Suncoast, as described above.

110. Plaintiffs and Class Members seek declaratory judgment that Suncoast's data security practices were not reasonable or adequate and caused the Data Breach under FDUTPA, as well as injunctive relief enjoining the above described wrongful acts and practices of Suncoast

and requiring Suncoast to employ and maintain industry accepted standards for data management and security, including, but not limited to, proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing. Fla. Stat. § 501.211(1).

111. Additionally, Plaintiffs and Class Members make claims for actual damages, attorneys' fees and costs. Fla. Stat. §§ 501.2105, 501.211(2).

COUNT II
Negligence
On behalf of Plaintiffs and the Class

112. Plaintiffs reallege paragraphs 1 through 100 above as if fully set forth herein. Plaintiffs bring this claim on behalf of the Class set forth above.

113. Suncoast had a duty to exercise reasonable care and protect and secure Plaintiffs' and Class Members' Personal Information. This duty exists at common law and is also codified under Federal law (*see*, *e.g.*, FTCA, FCRA, and HIPAA) and Florida law (*see*, *e.g.*, Fla. Stat. §§ 456.057, 501.171).

114. Through its acts and omissions, Suncoast breached its duty to use reasonable care to protect and secure Plaintiffs' and Class Members' Personal Information by employing substandard or non-existent data and cybersecurity protocols.

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

116. It was reasonably foreseeable, particularly given legal mandates governing health data protection and the growing number of data breaches of health information, that the failure to

reasonably protect and secure Plaintiffs' and Class Members' Personal Information would result in an unauthorized third-party gaining access to Suncoast's networks, databases, and computers that stored or contained Plaintiffs' and Class Members' Personal Information.

117. Plaintiffs' and Class Members' Personal Information constitutes personal property that was stolen due to Suncoast's negligence, resulting in harm, injury and damages to Plaintiffs and Class Members.

118. Suncoast's negligence directly and proximately caused the unauthorized access and disclosure of Plaintiffs' and Class Members' unencrypted Personal Information and Plaintiffs and Class Members have suffered and will continue to suffer damages as a result of Suncoast's conduct. Plaintiffs and Class Members seek damages and other relief as a result of Suncoast's negligence.

COUNT III
Breach of Express Contract
On behalf of Plaintiffs and the Class

119. Plaintiffs reallege paragraphs 1 through 100 above as if fully set forth herein. Plaintiffs bring this claim on behalf of the Class set forth above.

120. Suncoast provides medical services to Plaintiffs and Class Members pursuant to the terms of its contracts, which all were a party to, including agreements regarding the handling of their confidential Personal Information in accordance with Suncoast's policies, practices, and applicable law. Plaintiffs are not in possession of these contracts but believe these contracts are in the possession of Suncoast. As consideration, Plaintiffs and Class Members paid money to Suncoast and/or their insurers for medical services (or, in the case of Plaintiff Reardon, to a predecessor in interest who, on information and belief, transferred that contract to Suncoast). Accordingly, Plaintiffs and Class Members paid Suncoast to securely maintain and store their

Personal Information. Suncoast violated these contracts by failing to employ reasonable and adequate security measures to secure Plaintiffs' and Class Members' Personal Information and by disclosing it for purposes not required or permitted under the contracts.

121. Plaintiffs and Class Members have been damaged by Suncoast's conduct, including by paying for data and cybersecurity protection that they did not receive, as well as by incurring the harms and injuries arising from the Data Breach now and in the future.

COUNT IV
Breach of Implied Contract In Fact
On behalf of Plaintiffs and the Class

122. Plaintiffs reallege paragraphs 1 through 100 above as if fully set forth herein. Plaintiffs bring this claim on behalf of the Class set forth above. This Count is plead in the alternative to Count III (express contract).

123. Suncoast provides medical services to Plaintiffs and Class Members. Plaintiffs and Class Members also formed an implied contract with Suncoast regarding the provision of those services through their collective conduct, including by Plaintiffs and Class Members paying for medical goods and services from Suncoast and by Suncoast's performance of and sale of medical goods and services, regarding the handling of their confidential Personal Information in accordance with Suncoast's policies, practices, and applicable law. As consideration, Plaintiffs and Class Members paid money to Suncoast and/or their insurers for medical services (or, in the case of Plaintiff Reardon, to a predecessor in interest who, on information and belief, transferred that contract to Suncoast). Accordingly, Plaintiffs and Class Members paid Suncoast to securely maintain and store their Personal Information. Suncoast violated these contracts by failing to employ reasonable and adequate security measures to secure Plaintiffs' and Class Members'

Personal Information and by disclosing it for purposes not required or permitted under the contracts or agreements.

124. Plaintiffs and Class Members have been damaged by Suncoast's conduct, including by paying for data and cybersecurity protection that they did not receive, as well as by incurring the harms and injuries arising from the Data Breach now and in the future.

COUNT V
Invasion of Privacy (Electronic Intrusion)
On behalf of Plaintiffs and the Class

125. Plaintiffs reallege paragraphs 1 through 100 as if fully set forth herein. Plaintiffs bring this claim on behalf of the Class set forth above.

126. Plaintiffs and Class Members maintain a privacy interest in their Personal Information, which is private, confidential information that is also protected from disclosure by applicable laws set forth above. Plaintiffs' and Class Members' Personal Information was contained, stored, and managed electronically in Suncoast's records, computers, and databases that was intended to be secured from unauthorized access to third-parties because it contained highly sensitive, confidential matters regarding Plaintiffs' and Class Members' identities, unique identification numbers, medical histories, and financial records that were only shared with Suncoast (or, in the case of Plaintiff Reardon, to a predecessor in interest who, on information and belief, transferred that Personal Information to Suncoast) for the limited purpose of obtaining and paying for healthcare, medical goods and services. Additionally, Plaintiffs' and Class Members' Personal Information, when contained in electronic form, is highly attractive to criminals who can nefariously use their Personal Information for fraud, identity theft, and other crimes without their knowledge and consent.

127. Suncoast's disclosure of Plaintiffs' and Class Members' Personal Information to unauthorized third-parties as a result of its failure to adequately secure and safeguard their Personal Information is offensive to a reasonable person. Suncoast's disclosure of Plaintiffs' and Class Members' Personal Information to unauthorized third-parties permitted the physical and electronic intrusion into Plaintiffs' and Class Members' private quarters where their Personal Information was stored and disclosed private facts about their health into the public domain.

128. Plaintiffs and Class Members have been damaged by Suncoast's conduct, including by paying for data and cybersecurity protection that they did not receive, as well as by incurring the harms and injuries arising from the Data Breach now and in the future.

COUNT VI
Unjust Enrichment
On behalf of Plaintiffs Potter and Solomon and the Class

129. Plaintiffs reallege paragraphs 1 through 100 above as if fully set forth herein. Plaintiffs bring this claim on behalf of the Class set forth above.

130. Plaintiffs and Class Members conferred a benefit on Suncoast by paying for data and cybersecurity procedures to protect their Personal Information that they did not receive.

131. This conferral of benefit was not incidental to Plaintiffs' and Class Members' treatment—Plaintiffs and Class Members expected that Suncoast would ensure that their Personal Information would remain secure and not be disclosed to unauthorized third parties.

132. Suncoast has retained the benefits of its unlawful conduct including the amounts received for data and cybersecurity practices that it did not provide. Due to Suncoast's conduct alleged herein, it would be unjust and inequitable under the circumstances for Suncoast to be permitted to retain the benefit of its wrongful conduct.

133. Plaintiffs and the Class Members are entitled to full refunds, restitution and/or damages from Suncoast and/or an order of this Court proportionally disgorging all profits, benefits, and other compensation obtained by Suncoast from its wrongful conduct. If necessary, the establishment of a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation may be created.

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

COUNT VII
Breach of Confidence
On behalf of Plaintiffs Potter and Solomon and the Class

135. Plaintiffs reallege paragraphs 1 through 100 above as if fully set forth herein. Plaintiffs bring this claim on behalf of the Class set forth above.

136. At all times during Plaintiffs' and Class Members' relationship with Suncoast, Suncoast was fully aware of the confidential and sensitive nature of Plaintiffs' and Class Members' Personal Information.

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

138. Plaintiffs and Class Members provided their Personal Information to Suncoast with the explicit and implicit understandings that Suncoast would protect and not permit Personal Information to be disseminated to any unauthorized parties.

139. Plaintiffs and Class Members also provided their Personal Information to Suncoast with the explicit and implicit understandings that Suncoast would take precautions to protect such Personal Information from unauthorized disclosure.

140. Suncoast voluntarily received in confidence Plaintiffs' and Class Members' Personal Information with the understanding that the Personal Information would not be disclosed or disseminated to the public or any unauthorized third parties.

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

142. As a direct and proximate cause of Suncoast's actions and/or omissions, Plaintiffs and Class Members have suffered damages.

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

144. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Suncoast's unauthorized disclosure of Plaintiffs' and Class Members' Personal Information.

145. As a direct and proximate result of Suncoast's breaches of confidence, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual

identity theft; (ii) the compromise, publication, and/or theft of their Personal Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information; (iv) lost opportunity costs associated with effort expended to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from medical fraud, financial fraud, and identity theft; (v) costs associated with placing freezes on credit reports; (vi) the continued risk to their Personal Information, which remain in Suncoast's possession and is subject to further unauthorized disclosures so long as Suncoast fails to undertake appropriate and adequate measures to protect the Personal Information of patients in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Personal Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

146. As a direct and proximate result of Suncoast's breaches of confidence, Plaintiffs and Class Members have suffered and will continue to suffer injury and/or harm.

COUNT VIII
Breach of Fiduciary Duty
On behalf of Plaintiffs and the Class

147. Plaintiffs reallege paragraphs 1 through 100 above as if fully set forth herein. Plaintiffs bring this claim on behalf of the Class set forth above.

148. In light of their special relationship, Suncoast has become the guardian of Plaintiffs' and Class Members' Personal Information. Suncoast has become a fiduciary, created by its undertaking and guardianship of patient Personal Information, to act primarily for the benefit of their patients, including Plaintiffs and Class Members. This duty included the obligation to

safeguard Plaintiffs' and Class Members' Personal Information and to timely notify them in the event of a data breach.

149. Suncoast has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of their relationship. Suncoast has breached its fiduciary duties owed to Plaintiffs and Class Members by failing to:

(a) properly encrypt and otherwise protect the integrity of the system containing Plaintiffs' and Class Members' protected health information and other Personal Information;

(b) timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

(c) ensure the confidentiality and integrity of electronic protected health information Suncoast created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

(d) implement technical policies and procedures to limit access to only those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

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

(f) to identify and respond to suspected or known security incidents; 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);

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

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

(i) ensure compliance with the HIPAA security standard rules by their workforce in violation of 45 C.F.R. § 164.306(a)(94);

(j) improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, et seq.;

(k) effectively train all members of their workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of protected health information in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5)

(l) design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 C.F.R. § 164.530(c); and

(m) otherwise failing to safeguard Plaintiffs' and Class Members' Personal Information.

150. As a direct and proximate result of Suncoast's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including, but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Personal Information;

(iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Personal Information; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Personal Information, which remains in Suncoast's possession and is subject to further unauthorized disclosures so long as Suncoast fails to undertake appropriate and adequate measures to protect patient Personal Information in their continued possession; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Personal Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

151. As a direct and proximate result of Suncoast's breach of its fiduciary duty, Plaintiffs and Class Members have suffered and will continue to suffer injury and/or harm.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs on their own and behalf of all others similarly situated, pray for relief as follows:

A. For an Order certifying this case as a class action pursuant to Florida Rule of Civil Procedure 1.220, appointing Plaintiffs as Class Representatives, and the undersigned as Class Counsel;

B. Awarding monetary and actual damages and/or restitution, as appropriate, or nominal damages in the alternative;

C. Awarding declaratory and injunctive relief as permitted by law or equity to assure that the Class has an effective remedy, including enjoining Suncoast from continuing the unlawful practices as set forth above;

D. Awarding pre- and post-judgment interest to the extent allowed by the law;

E. Awarding all costs, experts' fees and attorneys' fees, expenses and costs of prosecuting this action; and

F. Such other and further relief as the Court may deem just and proper.

DATED: March 31, 2023

Respectfully Submitted,

/s/ Ryan J. McGee

MORGAN & MORGAN
COMPLEX LITIGATION GROUP
Ryan J. McGee, Esq. (FBN 064957)
RMcGee@ForThePeople.com
Francesca S. Kester, Esq. (FBN 1021991)
FKester@ForThePeople.co
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 222-4702

TURKE & STRAUSS LLP
Samuel J. Strauss*
sam@turkestrauss.com
Raina C. Borrelli*
raina@turkestrauss.com
613 Williamson St., Suite 201
Madison, WI 53703
Telephone (608) 237-1775
Facsimile: (608) 509-4423

Attorneys for Plaintiffs

* (*pro hac vice forthcoming*)

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on March 31, 2023, a true and accurate copy of the foregoing was filed with the Clerk of Court by using the electronic filing system which will serve via email this filing to all counsel of record.

/s/ Ryan J. McGee

MORGAN & MORGAN
COMPLEX LITIGATION GROUP
Ryan J. McGee, Esq. (FBN 064957)