UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

MARTHA CHANG, on behalf of herself and all others similarly situated, Plaintiff, v. LINCARE HOLDINGS INC., Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff, Martha Chang ("Plaintiff"), through her attorneys, brings this Class Action Complaint against the Defendant, Lincare Holdings, Inc. ("Lincare" or "Defendant"), alleging as follows:

INTRODUCTION

1. Lincare, one of the leading respiratory care providers in the United States operating in approximately 1,000 locations, lost control over its patients' highly sensitive medical and personal information in a data breach by cybercriminals ("Data Breach"). The Data Breach compromised the personally identifiable information ("PII") and personal health information ("PHI") of patients in its system, meaning patients are at risk of identity theft and harm. Cybercriminals could steal

patient data because Lincare did not adequately protect and secure patient PII and PHI, leaving the data an unguarded target for theft and misuse. Ms. Chang was a victim of the Data Breach and brings this Class Action on behalf of herself and all patients harmed by Lincare's conduct.

2. On September 26, 2021, Lincare learned that cybercriminals had breached its data systems and potentially accessed patients' PII and PHI. Lincare internally investigated the breach over nine months but has failed to identify exactly what the cybercriminals stole and from which patients. But the investigation did reveal that hackers started accessing Lincare's data systems on September 10, 2021 and had access to Lincare's systems through September 29, 2021.

3. Due to Lincare's inability to detect and prevent the Data Breach earlier, cybercriminals had access to patients' highly sensitive PII and PHI, including patient "first and last names, addresses, Lincare account numbers, date of birth, medical information, which may include information concerning medical treatments individuals received such as provider name, dates of service, diagnosis/procedures, and/or account or record numbers, health insurance information, and/or prescription information." Lincare also reported that in some circumstances, patient Social Security numbers may have been impacted.

4. Lincare is well-versed in data security matters, having previously experienced a data breach that compromised its employees' PII.

5. Lincare's inability to (i) safeguard patients' highly sensitive PII and PHI; (ii) determine the scale of the Data Breach; and (iii) promptly notify its patients of the breach violates Florida law and Lincare's implied contract with patients to safeguard their PII and PHI.

6. Ms. Chang and class members face a lifetime risk of identity theft due to the nature of the information lost, including patients' dates of birth and Social Security numbers, which they cannot change.

7. Lincare's harmful conduct has injured Ms. Chang and class members in multiple ways, including: (i) the lost or diminished value of their PII and PHI; (ii) costs associated with the prevention, detection, and recovery from identity theft, tax fraud, and other unauthorized use of their data; (iii) lost opportunity costs to mitigate the Data Breach's consequences, including lost time; and (iv) emotional distress associated with the loss of control over their highly sensitive PII and PHI.

8. Lincare's failure to protect patients' PII and PHI violates Florida law and harms hundreds of thousands of patients, causing Ms. Chang to seek relief on a class wide basis.

PARTIES

9. Plaintiff, Martha Chang is a resident and citizen of Missouri. Ms. Chang intends to remain domiciled in Missouri indefinitely and maintains her true, fixed, and permanent home in that state.

10. Lincare is a Delaware corporation registered to do business in the state of Florida with its principal place of business located at 19387 US 19 N., Clearwater, Florida 33764.

JURISDICTION & VENUE

11. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action in which the amount in controversy exceeds $5 million, exclusive of costs and interest, there are more than 100 members in the proposed class, and at least one class member is a citizen of a different state than Lincare, establishing minimal diversity.

12. This Court has personal jurisdiction over Lincare because it is registered to do business in Florida and its headquarters are in Clearwater, Florida.

13. Venue is proper in this Court under 28 U.S.C. §§ 1391 because a substantial part of the alleged wrongful conduct and events giving rise to the claims occurred in this District and because Lincare conducts business in this District.

FACTUAL ALLEGATIONS

A. Lincare

14. Lincare is a leading provider of in-home respiratory care providing oxygen, durable medical equipment and other respiratory care products and services to patients in their homes, nursing homes and at hundreds of Lincare centers across the country.

15. Upon information and belief, Lincare operates over 1,000 Lincare centers and provides services to hundreds of thousands of patients.

16. In exchange for its services, Lincare requires its patients to provide their highly sensitive PII and PHI, including their name, address, date of birth, Social Security number, medical record number, current/former member ID number, claims information, diagnosis and/or prescription information.

17. Lincare promises to safeguard patients' PII and PHI as part of its services, providing patients its "Company Privacy Policy" (the "Privacy Notice").[1]

18. The Privacy Notice explains how Lincare collects patient data as part of its services:

> • **Personally Identifiable Information:** This is information which you provide to us which personally identifies you, such as your name, postal or email address, phone number, billing information, date of birth, personally identifiable Health Information, etc. Health Information that you may provide to us includes but is not limited to any and all information, transmitted or maintained in electronic form, about your past, present, or future health or condition, treatment, medications, insurance benefits or other data that identifies you, collected and maintained by us, if you have registered to use an App or other Site (in which you provide and permit us to collect your Health Information in connection with a program in which you participate or services you receive from Company).By using any Site in which you disclose your Personally Identifiable Information, including your personally identifiable Health Information, you consent to and authorize us to receive, view, display, use, disclose, transmit and maintain Health Information on your behalf in connection with the ongoing support and services provided to you.

19. Lincare's Privacy Notice recognizes Lincare's duty to secure and maintain patient PII and Health Information and use it only in delivering Lincare's

[1] *See* Lincare's Privacy Notice, https://www.lincare.com/en/policies/privacy (last visited June 24, 2022).

services:[2]

HOW COMPANY USES INFORMATION

We use your Personally Identifiable Information to provide you with information and services you requested, and if applicable, we use your Health Information to provide you with all of the support and services offered through a program in which you registered through a Site. We will use your email address, without further consent, for administrative purposes, for customer service purposes, to address intellectual property infringement, rights of privacy, or defamation issues. If you interact with us via social media (see more below in OTHER SITES AND SENDING INFORMATION TO THIRD PARTIES), we may also use your Personally Identifiable Information to respond to your inquiries or comments, or to deliver advertisements and social media notifications about our brand, products, or services. We may also tailor our advertising on social media to send you more practical product or service recommendations and offers.

20. Ms. Chang and the proposed class are current and former Lincare patients.

21. As a condition of providing treatment, Lincare required Ms. Chang and the proposed class to provide their PII and PHI.

22. Lincare then collected and maintained patients' PII and PHI in its computer systems.

23. In collecting and storing patients' PII and PHI, Lincare implied that it would protect and maintain their data according to state and federal law and its Privacy Notice.

24. Ms. Chang and the proposed class relied on Lincare's representations in agreeing to provide their PII and PHI.

[2] *Id.*

B. Lincare fails to safeguard patients' PII and PHI

25. On September 10, 2021, Lincare lost control of patients' PII and PHI to cybercriminals in the Data Breach. Due to inadequate systems to safeguard patient data, Lincare was unaware of the breach for over two weeks, allowing cybercriminals to pilfer patients' PII and PHI undetected.

26. On September 26, 2021, Lincare finally discovered the Data Breach and allegedly began taking measures to stop it as of September 29, 2021. But through an internal investigation, Lincare was unable to determine the exact information cybercriminals stole and from which patients.

27. It took Lincare more than nine months –*until mid-June 2022*—to alert Ms. Chang that her PHI and PII may have been compromised in the Data Breach. On or about June 17, 2022, Ms. Chang learned about the Data Breach after Lincare issued a Notice of Security Incident ("Breach Notice"). A true and correct copy of the Breach Notice is attached as **Exhibit A**.

28. The Breach Notice reiterated that Lincare is "aware of how important personal information nis to patients and their loved ones."

29. The Breach Notice explained that Lincare lost control over "patient personal information," which included names, addresses, account information, dates of birth, medical information, health insurance information and in some cases Social Security numbers.

30. The Breach Notice said Lincare regretted "any inconvenience that this incident may have caused." It further stated Lincare was attempting to notify patients impacted by the Data Breach and was offering complimentary credit monitoring and identify theft protection.

31. The Breach Notice stated Lincare had enlisted cybersecurity experts to assist in the investigation and that it notified law enforcement of the Data Breach.

32. However, recognizing the severity of what occurred, Lincare also advised its patients to "remain vigilant against incidents of identify theft and fraud, to review all claims information from health insurance providers and to monitor credit reports and financial statements for suspicious activity." **Exh. A.**

33. This is not Lincare's first experience with data security incidents. In February of 2017, the PII of Lincare's employees was compromised in a data breach, resulting in a class-wide settlement of their data breach claims in *Giancola et. al v. Lincare Holdings Inc*., Case 8:17-CV-2427-VMA-AAS (M.D. Fla. Dec. 7, 2018).

34. On information and belief, despite its previous experience with cybersecurity failures, Lincare failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over patients' PII and PHI. Lincare's negligence is evidenced by its failure to recognize the Data Breach for over two weeks while cybercriminals had access to patient data, meaning Lincare had no effective means to detect and prevent

attempted data breaches. Further, the Breach Notice—sent to patients *more than nine months after* the Data Breach was discovered—makes clear that Lincare cannot even determine the full scope of the Data Breach, as it has been unable to determine exactly what information was stolen and when.

C. Plaintiff's experience

35. Ms. Chang has been a Lincare patient for more than ten years .

36. As a condition of receiving Lincare's services, Lincare requires Ms. Chang to provide her PII and PHI.

37. Since becoming a Lincare customer, Ms. Chang has provided Lincare her PII and PHI to purchase Lincare's services.

38. Ms. Chang believed, as part of her payments to Lincare for treatment and services, that those payments included amounts for data security. Had Ms. Chang known that Lincare did not utilize reasonable data security measures, she would have paid less for those treatments and services.

39. On or about June 17, 2022, Ms. Chang received notice from Lincare that her PII and PHI were compromised by the Data Breach.

40. In response, Ms. Chang has spent considerable time and effort monitoring her accounts to protect herself from additional identity theft. Ms. Chang fears for her personal financial security and uncertainty over what medical information was revealed in the Data Breach. She is experiencing feelings of anxiety,

sleep disruption, stress, and fear 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 is contemplated and addressed by law.

41. Lincare's proposed fix, a credit monitoring service, is inadequate to address Ms. Chang's losses, as she faces a risk of identity theft for the rest of her life.

42. Had Ms. Chang known that Lincare does not adequately protect PII and PHI, she would not have transacted with Lincare. Furthermore, Plaintiff's sensitive PII and PHI remains in Lincare's possession without adequate protection against known threats, exposing Ms. Chang to the prospect of additional harm in the event Lincare suffers another data breach.

D. Ms. Chang and the proposed class face significant risk of identity theft

43. Ms. Chang and members of the proposed class have suffered injury from the misuse of their PII and PHI that can be directly traced to Lincare.

44. The ramifications of Lincare's failure to keep Plaintiff's and the Class's PII and PHI secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, or other information, without permission, to commit fraud or other crimes.

45. According to experts, one out of four data breach notification recipients become a victim of identity fraud.

46. Because Lincare failed to prevent the Data Breach, Ms. Chang 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 PII and PHI are used;

b. The diminution in value of their PII and PHI;

c. The compromise and continuing publication of their PII and PHI;

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 trying 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 PII and PHI; and

h. The continued risk to their PII and PHI, which remains in the possession of Lincare and is subject to further breaches so long as Lincare fails to

undertake the appropriate measures to protect the PII and PHI in their possession.

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

48. The value of Plaintiff's and the proposed Class's PII and PHI on the black market is considerable. Stolen PII and PHI trades on the black market for years, and criminals often post stolen private information openly on various "dark web" internet websites, like Marketo, making the information publicly available, for a fee.

49. It can take victims years to spot identity or PII and PHI theft, giving criminals time to sell that information for cash.

50. One such example of criminals using PII and PHI for profit is the development of "Fullz" packages.

51. Cybercriminals can cross-reference multiple sources of PII and PHI to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

52. The development of "Fullz" packages means that stolen PII and PHI from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's 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 PII and PHI stolen by the cybercriminals 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 Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and other members of the proposed Class's stolen PII and PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

53. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, leading to more than $3.5 billion in losses to individuals and business victims.

54. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."

55. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

56. Along with out-of-pocket expenses that can exceed thousands of dollars for the victim of new account identity theft, and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their PHI. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continually monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

57. Further complicating the issues faced by victims of identity theft, data thieves may wait years before trying to use the stolen PII and PHI. To protect themselves, Plaintiff and the proposed Class will need to remain vigilant against unauthorized data use for years or even decades to come.

58. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner, Pamela Jones Harbour, stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."

59. The FTC has also issued several guidelines for businesses that highlight reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making. According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.

60. According to the FTC, unauthorized PHI disclosures are extremely damaging to consumers' finances, credit history, and reputation, and can take time, money, and patience to resolve the fallout. The FTC treats 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(a) of the FTC Act.

61. To that end, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. *See In the matter of Lookout Services, Inc.*, No. C-4326, ⁋ 7 (June 15, 2011) ("[Defendant] allowed users to bypass authentication procedures" and "failed to employ sufficient measures

to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ¶ 7 (Mar. 7, 2006) ("[Defendant] failed to employ sufficient measures to detect unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (May 20, 2010) ("[Defendant] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between instore networks . . ."). These orders, which all preceded the Data Breach, further clarify the measures businesses must take to meet their data security obligations.

E. Lincare Failed to Adhere to HIPAA

62. 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.

63. 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.

64. The Data Breach itself resulted from a combination of inadequacies showing Lincare failed to comply with safeguards mandated by HIPAA. Lincare'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 Lincare's 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 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).

F. Lincare Failed to Adhere to FTC Guidelines

65. 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 Lincare, should employ to protect against the unlawful exposure of Personal Information.

66. 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.

67. 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.

68. The FTC recommends that companies not maintain PHI 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.

69. 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.

70. Lincare's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PHI constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

CLASS ACTION ALLEGATIONS

71. Ms. Chang sues on behalf of herself and the proposed class ("Class"), defined as follows:

> All individuals residing in the United States whose personal information was compromised in the Data Breach disclosed by Lincare in June 2022.

Excluded from the Class are Lincare, its agents, affiliates, parents, subsidiaries, any entity in which Lincare has a controlling interest, any Lincare officer or director, any

successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

72. Ms. Chang reserves the right to amend the class definition.

73. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. Ms. Chang is a representative of the proposed Class consisting of thousands of members—far too many to join in a single action;

b. **Ascertainability**. Class members are readily identifiable from information in Lincare's possession, custody, and control;

c. **Typicality**. Ms. Chang's claims are typical of Class member's claims as each arises from the same Data Breach, the same alleged negligence and statutory violations by Lincare, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Ms. Chang will fairly and adequately protect the proposed Class's interests. Her interests do not conflict with Class members' interests, and she 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**. Ms. Chang's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding

can answer for all Class members. Indeed, it will be necessary to answer the following questions:

i. Whether Lincare had a duty to use reasonable care in safeguarding Ms. Chang and the Class's PII and PHI;

ii. Whether Lincare 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 Lincare was negligent in maintaining, protecting, and securing PII and PHI;

iv. Whether Lincare breached contractual promises to safeguard Ms. Chang and the Class's PII and PHI;

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

vi. Whether Lincare's Breach Notice was reasonable;

vii. Whether the Data Breach caused Ms. Chang and the Class injuries;

viii. What the proper damages measure is;

ix. Whether Lincare violated the statutes alleged in this complaint; and

x. Whether Ms. Chang and the Class are entitled to damages, treble damages, or injunctive relief.

74. 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.

FIRST CLAIM FOR RELIEF
Negligence
(On Behalf of Plaintiff and the Class)

75. Plaintiff incorporates all previous paragraphs as if fully set forth below.

76. Plaintiff and members of the Class entrusted their PII and PHI to Defendant. Defendant owed to Plaintiff and other members of the Class a duty to exercise reasonable care in handling and using the PII and PHI in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that happened, and to promptly detect attempts at unauthorized access.

77. Defendant owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their PII and PHI in accordance with state-of-the-art industry standards for data security would result in the compromise of that PII and PHI—just like the Data Breach that

ultimately happened. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and members of the Class's PII and PHI by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PII and PHI was stored, used, and exchanged, and those in its employ who made that happen.

78. Defendant owed to Plaintiff and members of the Class a duty to notify them within a reasonable time frame of any breach to the security of their PII and PHI. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and members of the Class to respond appropriately to protect their PII and PHI, 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.

79. Defendant owed these duties to Plaintiff and members of the Class 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 protocols. Defendant actively sought and obtained Plaintiff's and members of the Class's PII and PHI for medical services. Plaintiff and members of the Class needed to provide their PII and PHI to Defendant

to receive medical services from Defendant, and Defendant retained that information.

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

81. PII and PHI is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII and PHI of Plaintiff and members of the Class's and the importance of exercising reasonable care in handling it.

82. 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 PII and PHI of Plaintiff and members of the Class which actually and proximately caused the Data Breach and Plaintiff's and members of the Class's injury.

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

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

85. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff's and members of the Class's actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII and PHI by criminals, improper disclosure of their PII and PHI, lost benefit of their bargain, lost value of their PII and PHI, 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.

SECOND CLAIM FOR RELIEF
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

86. Plaintiff incorporates all previous paragraphs as if fully set forth below.

87. Defendant had a duty to protect and maintain and provide adequate data security to maintain Plaintiff and the Class's PII and PHI under § 5 of the FTC Act, 15 U.S.C. § 45.

88. The FTC Act prohibits unfair business practices affecting commerce, which the FTC has interpreted to include a failure to use reasonable measures to

safeguard PII.

89. Defendants' violation of these duties is negligence *per se* under Florida law.

90. Plaintiff and the proposed Class are included in the class of persons that the FTC Act was intended to protect.

91. The harm the Data Breach caused is the type the FTC Act was intended to guard against.

92. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence per se.

93. Pursuant to HIPAA (42 U.S.C. § 1302d, et seq.), Defendant had a duty to implement reasonable safeguards to protect Plaintiff's and Class members' PHI.

94. Pursuant to HIPAA, Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 C.F.R. § 164.304 definition of encryption).

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

96. The harm that occurred as a result of the Data Breach is the type of

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

97. Defendant breached its duties to Plaintiff and the Class under HIPAA, by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' PHI.

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

99. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

100. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PHI.

101. Had Plaintiff and members of the Class known that Defendant did not adequately protect their PHI, Plaintiff and members of the Class would not have

entrusted Defendant with their PHI.

102. Defendant's negligence *per se* caused Plaintiff and the proposed Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII and PHI by criminals, improper disclosure of their PII and PHI, lost benefit of their bargain, lost value of their PII and PHI, 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.

THIRD CLAIM FOR RELIEF
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

103. Plaintiff incorporates all previous paragraphs as if fully set forth below.

104. Defendant offered to provide goods and services to Plaintiff and members of the Class in exchange for payment.

105. Defendant also required Plaintiff and the members of the Class to provide Defendant with their PII and PHI to receive services.

106. In turn, and through the Privacy Notice, Defendant agreed it would not disclose the PHI it collects from patients to unauthorized persons. Defendant also impliedly promised to maintain safeguards to protect its patients' PII and PHI.

107. Defendant recognized its implied promise in its Breach Notice, stating that Defendant was "committed to protecting the confidentiality and security of the information we maintain," including patient PII and PHI.

108. Plaintiff and the members of the Class accepted Defendant's offer by providing PII and PHI to Defendant in exchange for receiving Defendant's goods and services and then by paying for and receiving the same.

109. Implicit in the parties' agreement was that Defendant would provide Plaintiff and members of the Class with prompt and adequate notice of all unauthorized access or theft of their PII and PHI.

110. Plaintiff and the members of the Class would not have entrusted their PII and PHI to Defendant without such agreement with Defendant.

111. Defendant materially breached the contract(s) it had entered with Plaintiff and members of the Class by failing to safeguard such information and failing to notify them promptly of the intrusion into its computer systems that compromised such information. Defendant also breached the implied contracts with Plaintiff and members of the Class by:

a. Failing to properly safeguard and protect Plaintiff's and members of the Class's PII and PHI;

b. Violating industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement;

c. Failing to ensure the confidentiality and integrity of electronic PII and PHI that Defendant created, received, maintained, and transmitted in violation of 45 C.F.R. § 164.306(a)(1).

112. The damages sustained by Plaintiff and members of the Class as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

113. Plaintiff and members of the Class have performed under the relevant agreements, or such performance was waived by the conduct of Defendant.

114. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose on each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract along with its form.

115. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

116. Defendant failed to advise Plaintiff and members of the Class of the Data Breach promptly and sufficiently.

117. In these and other ways, Defendant violated its duty of good faith and fair dealing.

118. Plaintiff and members of the Class have sustained damages because of Defendant's breaches of its agreement, including breaches of it through violations of the covenant of good faith and fair dealing.

FOURTH CLAIM FOR RELIEF
Unjust Enrichment

(On Behalf of Plaintiff and the Class)

119. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

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

121. Plaintiff and members of the Class conferred a monetary benefit upon Defendant in the form of monies paid for treatment services.

122. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff and members of the Class. Defendant also benefited from the receipt of Plaintiff's and members of the Class's PII and PHI, as this was used to facilitate payment and treatment services.

123. As a result of Defendant's conduct, Plaintiff and members of the Class suffered actual damages in an amount equal to the difference in value between their purchases made with reasonable data privacy and security practices and procedures that Plaintiff and members of the Class paid for, and those purchases without unreasonable data privacy and security practices and procedures that they received.

124. Under principals of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and members of the Class because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures for itself that Plaintiff and members of the Class paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

125. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged herein.

PRAYER FOR RELIEF

Plaintiff and members of 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 Ms. Chang and the proposed Class, appointing Ms. Chang as class representative, and appointing her counsel to represent the Class;

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

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

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

E. Awarding Ms. Chang and the Class damages that include compensatory, exemplary, punitive damages, and statutory damages, including pre- and post-judgment interest, in an amount to be proven at trial;

F. Awarding restitution and damages to Plaintiff 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 Plaintiff 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.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

RESPECTFULLY SUBMITTED AND DATED this 28th day of June, 2022.

/s/Avi R. Kaufman
Avi R. Kaufman (Florida Bar no. 84382)
kaufman@kaufmanpa.com
Rachel E. Kaufman (Florida Bar no. 87406)
rachel@kaufmanpa.com
KAUFMAN P.A.
237 S Dixie Hwy, 4th Floor
Coral Gables, FL 33133
Telephone: (305) 469-5881

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

Attorneys for Plaintiff