UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

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

Plaintiff, Victor Juarez ("Plaintiff"), through his attorneys, brings this Class Action Complaint against the Defendant, Lincare Holdings, Inc. ("Lincare" or "Defendant"). The allegations contained herein are based on Plaintiff's personal knowledge of facts pertaining to himself and upon information and belief, including further investigation conducted by Plaintiff's counsel.

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. As a result, patients are at risk of identity theft and harm. Lincare did not adequately protect and secure patient PII and PHI, leaving the data an unguarded target for theft and misuse. Lincare's failures allowed cybercriminals to steal patient data.

2. Plaintiff Juarez was a victim of the Data Breach and brings this Class Action lawsuit on behalf of himself and all California citizens who are current or former Lincare patients and victims of the Data Breach.

3. On September 26, 2021, Lincare learned that cybercriminals breached its data systems and potentially accessed patients' PII and PHI. Lincare purportedly spent over nine months investigating the breach, but it has nonetheless failed to identify exactly what the cybercriminals stole and from which patients. The investigation did, however, reveal that hackers began accessing Lincare's data systems on September 10, 2021 and continued to have access to Lincare's systems through September 29, 2021.

4. As a result of Lincare's failure 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.

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

6. Lincare's failure 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 state and federal laws and Lincare's common law and contractual duty to safeguard its patients' PII and PHI.

7. Plaintiff Juarez and class members face a lifetime risk of identity theft due to the

nature of the compromised information, including patients' dates of birth and Social Security numbers, which they cannot change.

8. Lincare's harmful conduct has injured Plaintiff Juarez 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.

9. Lincare's failure to protect patients' PII and PHI violates federal and state laws and harms hundreds of thousands of patients, causing Plaintiff Juarez to seek relief on a class wide basis.

PARTIES

10. Plaintiff, Victor Juarez is a resident and citizen of California. Plaintiff Juarez intends to remain domiciled in California and maintains his true, fixed, and permanent home in Watsonville, California.

11. 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

12. 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.

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

14. 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 Plaintiff's claims occurred in this District and because Lincare conducts business in this District.

FACTUAL ALLEGATIONS

A. Lincare

15. 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 hundreds of Lincare centers across the country.

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

17. In exchange for its services, Lincare requires its patients—including Plaintiff Juarez and the proposed class—to provide their highly sensitive PII and/or 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.

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

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

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

- **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.

20. 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 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.

21. As a condition of providing treatment, Lincare required Plaintiff Juarez and the proposed class to provide their PII and PHI, which Lincare collected and maintained in its computer system.

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

[2] *Id.*

23. Plaintiff Juarez and the proposed class relied on Lincare's representations in agreeing to provide their PII and PHI.

B. Lincare Failed to Safeguard Patients' PII and PHI

24. On September 10, 2021, Lincare lost control of patients' PII and PHI to cybercriminals who carried out the Data Breach. As a result of Lincare's inadequate systems and its inability to safeguard patient data, Lincare was unaware of the breach for over two weeks. This gave cybercriminals ample time to pilfer patients' PII and PHI without interference or detection.

25. 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.

26. It took Lincare more than nine months to alert Plaintiff Juarez that his PHI and PII may have been compromised in the Data Breach. On or about June 28, 2022, Plaintiff Juarez learned about the Data Breach after Lincare issued a Notice of Data Breach ("Breach Notice").

27. The Breach Notice explained that Lincare lost control over "patient personal information," which included Plaintiff's and Class Members' names, addresses, account information, dates of birth, medical information, health insurance information and/or Social Security numbers.

28. 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.

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

30. 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."

31. 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).

32. 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. This demonstrates that Lincare did not have an adequate system in place to timely detect and prevent attempted data breaches. Lincare had no effective means to detect and prevent attempted data breaches. Further, the Breach Notice, which was not sent to patients until more than nine months after the Data Breach was discovered, demonstrates that Lincare cannot 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

33. Plaintiff Juarez was a patient at Watsonville Community Hospital in April 2020 and September 2021, and he became one of Lincare's customers when he received respiratory services from Lincare.

34. As a condition of receiving Lincare's services, Lincare required Plaintiff Juarez to provide his PII and PHI.

35. Since becoming a Lincare customer, Plaintiff Juarez has provided Lincare his PII and PHI to purchase Lincare's services.

36. Plaintiff Juarez believed, as part of his payments to Lincare for treatment and services, that those payments included amounts for data security. Had Plaintiff Juarez known that Lincare did not utilize reasonable data security measures, he would have paid less for those treatments and services or would have insisted that his PII and PHI not be stored in Lincare's system.

37. In June of 2022, Plaintiff Juarez received a notice letter from Lincare, dated June 21, 2022, informing him that his PII and PHI were compromised by the Data Breach.

38. In response, Plaintiff Juarez has spent considerable time and effort monitoring his accounts to protect himself from additional identity theft. Plaintiff Juarez fears for his personal financial security and uncertainty over what medical information was revealed in the Data Breach. He is experiencing feelings of anxiety, 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. Moreover, Plaintiff Juarez has experienced an increase in spam and phishing attempts since the Data Breach and believes that this activity is a result of the Data Breach based on the timing of these events.

39. Had Plaintiff Juarez known that Lincare does not adequately protect PII and PHI, he 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 Plaintiff Juarez to the prospect of additional harm in the event Lincare suffers another data breach.

D. Plaintiff Juarez and the Proposed Class Face Significant Risk of Identity Theft

40. Plaintiff Juarez and members of the proposed class have suffered injury from the misuse of their PII and PHI that can be directly traced to Lincare.

41. 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.

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

43. Because Lincare failed to prevent the Data Breach, Plaintiff Juarez and members of 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.

44. 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.

45. Plaintiff and Class Members' PII and PHI is valuable, and stolen PII and PHI is commonly traded on the black market for several years following a data breach. Criminals openly post stolen private information on various "dark web" internet websites and make the information publicly available for a fee.

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

47. One such example of criminals using PII and PHI for profit is the development of "Fullz" packages—a dossier that contains valuable data pertaining to a particular victim.

48. Cybercriminals can cross-reference multiple sources of PII and PHI to combine stolen data with other unregulated data that is available elsewhere. As a result, these "Fullz" packages are astonishingly complete in terms of scope and their degree of accuracy.

49. The development of "Fullz" packages means that stolen PII and PHI from the Data Breach can easily be used to identify Plaintiff and class members and link the stolen data to Plaintiff and class members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the 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 and class members' stolen PII and PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

50. 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.

51. The same report explains that "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Despite the urgency and importance of notifying patients of potential risks arising from the Data Breach, Lincare waited over nine months before it reported the Data Breach.

52. In addition to financial losses resulting from fraudulently opened accounts or misuse of existing accounts, victims of identity theft often suffer embarrassment, blackmail, harassments (in-person and/or online), and emotional distress.

53. Moreover, victims are forced to spend considerable time and effort repairing the damage caused by the theft of their PHI, including but not limited to, time spent reporting and correcting fraudulent information in their credit reports, continually monitoring their reports for future inaccuracies, closing existing bank/credit accounts, opening new ones, and disputing charges with creditors.

54. To make matters worse, data thieves may wait several years before attempting 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.

55. 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."

56. The FTC has also issued several guidelines for businesses that highlight reasonable data security practices. 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.

57. 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. To that end, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data.[3]

[3] *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

E. Lincare Failed to Adhere to HIPAA

58. HIPAA requires 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.

59. 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.

60. The Data Breach resulted from a combination of inadequacies, which demonstrates that Lincare failed to comply with HIPAA's requirements. 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);

---

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.

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

61. According to the Federal Trade Commission ("FTC"), data security should be an important factor in every business decision. 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.

62. 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.[4]

63. The guidelines also recommend that businesses monitor their systems for large transmission of data and have a contingency plan ready in the event of a data breach.

64. 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.

65. 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.

[4] The FTC also 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.

CLASS ACTION ALLEGATIONS

66. Plaintiff Juarez brings this lawsuit on behalf of himself and the proposed class ("Class"), defined as follows:

> All individuals residing in California whose personal information was compromised, accessed, or viewed 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. Also excluded from the Class are all individuals who make a timely election to be excluded from this proceeding using the Court ordered protocol for opting out.

67. Plaintiff Juarez reserves the right to amend the definition of the proposed Class before the Court determines whether certification is appropriate.

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

a. **Numerosity**. The Class is so numerous that joinder of all members is impracticable. The Class includes thousands of individuals whose personal data was compromised by the Data Breach. The exact number of Class members is in the possession and control of Defendant and will be ascertainable through discovery.

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

c. **Typicality**. Plaintiff's claims are typical of the claims of the Class in that Plaintiff, like all Class members, had his personal data compromised, breached, and stolen in the Data Breach. Plaintiff and all Class Members were injured as a result of Lincare's

uniform misconduct, which is described throughout this Complaint, and assert the same claims for relief.

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

e. **Superiority.** Class action treatment is a superior method for the fair and efficient adjudication of the controversy. Such treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, or expense that numerous individual actions would engender. The benefits of proceeding through the class mechanism, including providing injured persons a method for obtaining redress on claims that could not practicably be pursued individually, substantially outweighs potential difficulties in management of this class action. Plaintiffs are unaware of any special difficulty to be encountered in litigating this action that would preclude its maintenance as a class action.

f. **Commonality**. Questions of law and fact common to the Class Members predominate over questions that may affect only individual Class Members because Defendant has acted on grounds generally applicable to the Class. Such generally applicable conduct is inherent in Defendant's wrongful conduct. The following questions of law and fact are common to the Class:

i. Whether Lincare had a duty to use reasonable care in safeguarding Plaintiff Juarez 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 Plaintiff Juarez 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 Plaintiff Juarez and the Class injuries;

viii. What the proper damages measure is;

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

x. Whether Plaintiff Juarez and the Class are entitled to damages, civil penalties, punitive damages, declaratory and/or injunctive relief.

69. Further, the damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

FIRST CLAIM FOR RELIEF
Violation of The California Confidentiality of Medical Information Act,
Cal. Civ. Code § 56, *et seq*.
(On Behalf of Plaintiff and the Class)

70. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained above.

71. Under the California Confidentiality of Medical Information Act, Civil Code §§ 56, *et seq*. (hereinafter referred to as the "CMIA"), "medical information" means "any

individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment." Cal. Civ. Code § 56.05

72. Additionally, Cal. Civ. Code § 56.05 defines "individually identifiable" as meaning that "the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the identity of the individual." Cal. Civ. Code § 56.05.

73. Under Cal. Civ. Code § 56.101(a) of the CMIA,

> (a) Every provider of health care, health care service plan, pharmaceutical company, or contractor who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the confidentiality of the information contained therein. Any provider of health care, health care service plan, pharmaceutical company, or contractor who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36.

Cal. Civ. Code § 56.101.

71. At all relevant times, Lincare was a health care contractor within the meaning of Civil Code § 56.05(d) because it is a "medical group, independent practice association, pharmaceutical benefits manager, or medical service organization and is not a health care service plan or provider of health care." In the alternative, Defendant is a health care provider within the meaning of Civil Code § 56.06(b), because it "offers software or hardware to consumers, including a mobile application or other related device that is designed to maintain medical information . . ." and maintains medical information as defined by Civil Code § 56.05.

72. Plaintiff and Class Members are Defendant's patients, as defined in Civil Code § 56.05(k).

73. Plaintiff and Class Members provided their personal medical information to Lincare.

74. At all relevant times, Defendant created, maintained, preserved, stored, abandoned, destroyed, or disposed of medical information in the ordinary course business.

75. As a result of the Data Breach, Defendant has misused, disclosed, and/or allowed third parties to access and view Plaintiff's and Class Members' personal medical information without their written authorization compliant with the provisions of Civil Code §§ 56, *et seq*. As a further result of the Data Breach, the confidential nature of the Plaintiff's medical information was breached as a result of Defendant's negligence.

76. Specifically, Defendant knowingly allowed and affirmatively acted in a manner that actually allowed unauthorized parties to access and view Plaintiff's and Class Members' PHI/PII, which was viewed and used when the unauthorized parties engaged in the above-described fraudulent activity. Defendant's misuse and/or disclosure of medical information regarding Plaintiff and Class Members constitutes a violation of Civil Code §§ 56.10, 56.11, 56.13, and 56.26.

77. As a direct and proximate result of Defendant's wrongful actions, inaction, omissions, and failure to exercise ordinary care, Plaintiff's and Class Members' PHI/PII was disclosed without written authorization.

78. By disclosing Plaintiff's and Class Members' Private Information without their written authorization, Defendant violated California Civil Code § 56, *et seq*., and its legal duty to protect the confidentiality of such information.

79. Defendant also violated Sections 56.06 and 56.101 of the California CMIA, which prohibit the negligent creation, maintenance, preservation, storage, abandonment, destruction or disposal of confidential personal medical information.

80. As a direct and proximate result of Defendant's wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff's and Class Members' personal medical information was viewed by, released to, and disclosed to third parties without Plaintiff's and Class Members' written authorization.

81. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violation of the CMIA, Plaintiff and Class Members are entitled to (i) actual damages, (ii) nominal damages of $1,000 per Plaintiff and Class Member, (iii) punitive damages of up to $3,000 per Plaintiff and Class Member, and (iv) attorneys' fees, litigation expenses and court costs under California Civil Code § 56.35.

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 Plaintiff Juarez and the proposed Class, appointing Plaintiff Juarez as class representative, and appointing his counsel to represent the Class;

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

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff Juarez 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 Plaintiff Juarez 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.

DEMAND FOR JURY TRIAL

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, Plaintiff, on behalf of himself and the proposed Class, demands a trial by jury on all issues so triable.

Dated: July 28, 2022

Respectfully submitted,

/s/ Jonathan B. Cohen

Jonathan B. Cohen
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
100 Garden City Plaza, Suite 500
Garden City, New York 11530
(212) 594-5300 (phone)
jcohen@milberg.com

Alexandra Honeycutt*
Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, Illinois 60606
Telephone: (847) 208-4585
ahoneycutt@milberg.com
gklinger@milberg.com

Attorneys for Plaintiff and Putative Class
**pro hac vice* forthcoming