UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

IN RE LINCARE HOLDINGS INC. DATA BREACH LITIGATION

Case No. 8:22-cv-1472-TPB-AAS

/

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs B.B., Martha Chang, Ronald Fudge, Victor Juarez, Cherry Merrell, George Miller, and Lisa Torres, individually, and on behalf of the proposed classes of similarly situated individuals ("Class Members") described below, bring this action for injunctive relief, and actual and statutory damages against Defendant Lincare Holdings Inc. and allege, upon personal knowledge as to their own actions and their counsel's investigations, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Representative Plaintiffs B.B., Martha Chang, Ronald Fudge, Victor Juarez, Cherry Merrell, George Miller, and Lisa Torres ("Representative Plaintiffs") bring this class action against Defendant Lincare Holdings, Inc. ("Defendant" or "Lincare") for its failure to properly secure and safeguard Representative Plaintiffs' and Class Members' Protected Health Information and personally identifiable information stored within Defendant's information network, including, without limitation, medical information such as information regarding medical treatments,

provider names, dates of service, diagnosis/procedure information, (these types of information, *inter alia*, being hereafter referred to, collectively, as "Protected Health Information" or "PHI"),[1] account numbers and/or record numbers, names, and dates of birth (these latter types of information, *inter alia*, being hereafter referred to, collectively, as "personally identifiable information" or "PII").[2]

2. With this action, Representative Plaintiffs seek to hold Defendant responsible for the harms it caused and will continue to cause Representative Plaintiffs and the countless other similarly situated persons in the massive and preventable cyberattack beginning as early as September 10, 2021 and discovered by Defendant on September 26, 2021, by which cybercriminals infiltrated Defendant's inadequately protected network servers and accessed highly sensitive PII/PHI and financial information which was being kept unprotected (the "Data Breach" or "Breach").

3. Representative Plaintiffs further seek to hold Defendant responsible for

[1] Protected Health Information ("PHI") is a category of information that refers to an individual's medical records and history, which is protected under the Health Insurance Portability and Accountability Act. *Inter alia*, PHI includes test results, procedure descriptions, diagnoses, personal or family medical histories, and data points applied to a set of demographic information for a particular patient. PHI is inclusive of and incorporates personally identifiable information.

[2] Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).

not ensuring that the PII/PHI was maintained in a manner consistent with industry standards, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy Rule (45 CFR, Parts 160 and 164(A) and (E)), the HIPAA Security Rule (45 CFR, Parts 160 and 164(A) and (C)), and other relevant standards.

4. While Defendant claims to have discovered the Breach as early as September 26, 2021, Defendant did not begin informing victims of the Data Breach until June 2022. Indeed, Representative Plaintiffs and Class Members were wholly unaware of the Data Breach until they received letters from Defendant informing them of it (the "Notice").[3]

5. Defendant acquired, collected, and stored Representative Plaintiffs' and Class Members' PII/PHI and/or financial information to facilitate the healthcare services Representative Plaintiffs and Class Members requested or received. Therefore, at all relevant times, Defendant knew, or should have known, that would its networks stored sensitive data, including Representative Plaintiffs' and Class Members' highly confidential PII/PHI.

6. HIPAA establishes obligations for the protection of individuals' medical records and other personal health information. HIPAA, generally, applies to health plans/insurers, health care clearinghouses, and those health care providers that

[3] https://www.lincare.com/-/media/project/lincare/files/security_notice.pdf (last accessed December 16, 2022); https://www.doj.nh.gov/consumer/security-breaches/documents/lincare-holdings-20220613.pdf (last accessed December 16, 2022).

conduct certain health care transactions electronically, and sets requirements for Defendant's maintenance of Representative Plaintiffs' and Class Members' PII/PHI. More specifically, HIPAA requires appropriate safeguards be maintained by organizations such as Defendant to protect the privacy of patient health information and sets limits and conditions on the uses and disclosures that may be made of such information without customer/patient authorization. HIPAA also gives a series of rights to patients over their PII/PHI, including rights to examine and obtain copies of their health records, and to request corrections thereto.

7. Additionally, the HIPAA Security Rule establishes national standards to protect individuals' electronic health information that is created, received, used, or maintained by a covered entity. The HIPAA Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic Protected Health Information.

8. By obtaining, collecting, using, and deriving a benefit from Representative Plaintiffs' and Class Members' PII/PHI, Defendant assumed legal and equitable duties to those individuals. These duties arise from HIPAA and other state and federal statutes and regulations as well as common law principles. Representative Plaintiffs do not bring claims in this action for direct violations of HIPAA, but charges Defendant with various legal violations merely predicated upon the duties set forth in HIPAA. HIPAA provides the standard of procedure by which

a medical provider must operate when collecting, storing, and maintaining Protected Health Information.

9. Defendant disregarded the rights of Representative Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Representative Plaintiffs' and Class Members' PII/PHI was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII/PHI of Representative Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party that seeks to profit off this disclosure by defrauding Representative Plaintiffs and Class Members in the future. Representative Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they are entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

10. Jurisdiction is proper in this Court under 28 U.S.C. §1332 (diversity jurisdiction). Specifically, this Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest

and costs, there are more than 100 members in the proposed class, and at least one other Class Member is a citizen of a state different from Defendant.

11. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in this Court under 28 U.S.C. §1367.

12. Defendant routinely conducts business in Florida, has sufficient minimum contacts in Florida, and has intentionally availed itself of this jurisdiction by marketing and selling products and services, and by accepting and processing payments for those products and services within Florida.

13. Venue is proper in this Court under 28 U.S.C. § 1391 because Defendant does business in this Judicial District.

PLAINTIFFS

14. Representative Plaintiff B.B. is an adult individual and, at all relevant times, a citizen and resident of the State of Missouri. Plaintiff B.B. has no intention of moving to a different state in the immediate future.

15. Representative Plaintiff Chang is an adult individual and, at all relevant times, a citizen and resident of the State of Missouri. Plaintiff Chang has no intention of moving to a different state in the immediate future.

16. Representative Plaintiff Fudge is an adult individual and, at all relevant times, a citizen and resident of the State of Alabama. Plaintiff Fudge has no intention of moving to a different state in the immediate future.

17. Representative Plaintiff Juarez is an adult individual and, at all relevant times, a citizen and resident of the State of California. Plaintiff Juarez has no intention of moving to a different state in the immediate future.

18. Representative Plaintiff Merrell is an adult individual and, at all relevant times, a citizen and resident of the State of Georgia. Plaintiff Merrell has no intention of moving to a different state in the immediate future.

19. Representative Plaintiff Miller is an adult individual and, at all relevant times, a citizen and resident of the State of New York. Plaintiff Miller has no intention of moving to a different state in the immediate future.

20. Representative Plaintiff Torres is an adult individual and, at all relevant times, a citizen and resident of the State of North Carolina. Plaintiff Torres has no intention of moving to a different state in the immediate future.

21. All Representative Plaintiffs are victims of the Data Breach.

22. Defendant received highly sensitive personal, medical, and financial information from all Representative Plaintiffs and Class Members in connection with the purchase of medical products from Defendant.

23. Representative Plaintiffs and Class Members received—and were "consumers" for purposes of obtaining—medical care from Defendant.

24. As required, in order to obtain services from Defendant, Representative Plaintiffs and Class Members provided Defendant with highly sensitive personal,

financial, health, and insurance information.

25. Data security is an essential element of any healthcare service where patients are required to provide their PII/PHI to obtain such services (much as confidentiality under an attorney-client relationship is essential to such services).

26. Because of the importance of maintaining the confidentiality of PII/PHI, Representative Plaintiffs and Class Members purchased data security and healthcare services from Defendant. Accordingly, Representative Plaintiffs and Class Members expected that a part of the monies they paid Defendant would be used for data security.

27. Had Representative Plaintiffs and Class Members known of Defendant's inadequate data security, they would not have purchased services from Defendant.

28. Representative Plaintiffs' PII/PHI was exposed in the Data Breach because Defendant stored and/or shared Representative Plaintiffs' PII/PHI and financial information. Their PII/PHI and financial information was within the possession and control of Defendant at the time of the Data Breach.

29. As a result, Representative Plaintiffs spent time dealing with the consequences of the Data Breach, which included and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self- monitoring their accounts, and

seeking legal counsel regarding their options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

30. Representative Plaintiffs suffered actual injury in the form of damages to and diminution in the value of their PII/PHI—a form of intangible property that they entrusted to Defendant, which was compromised in and as a result of the Data Breach.

31. Representative Plaintiffs suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and have anxiety and increased concerns for the loss of their privacy, as well as anxiety over the impact of cybercriminals accessing and using their PII/PHI and/or financial information.

32. Representative Plaintiffs are now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from their PII/PHI and financial information, in combination with their names, being placed in the hands of unauthorized third parties/criminals. This injury was worsened by Defendant's months-long delay in informing Representative Plaintiffs and Class Members about the Data Breach.

33. Following the Breach and recognizing that each Class Member is now subject to the present and continuing risk of identity theft and fraud, Defendant offered Representative Plaintiffs and Class Members identity theft protection through Kroll for twelve months. Such an offer is insufficient to protect

Representative Plaintiffs and Class Members from the lifetime risks each now face. As another element of damages. Representative Plaintiffs and Class Members seek a sum of money sufficient to provide to Representative Plaintiffs and Class Members identity theft protective services for their respective lifetimes.

34. Representative Plaintiffs have a continuing interest in ensuring that their PII/PHI and financial information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

DEFENDANT

35. Defendant is a Delaware corporation with a principal place of business located at 19387 US 19 N., Clearwater, Florida 33764.

36. Defendant offers a variety of medical products and services, such as cardiac monitoring services, durable medical equipment, oxygen therapy, nebulizer therapy, pharmacy services, and more. Its mission is "to set the standard for excellence, transforming the way respiratory care is delivered in the home."[4] Defendant's operation includes dozens of subsidiaries and partners across North America.[5]

[4] *See* https://www.lincare.com/en/ (last accessed Dec. 27, 2022).

[5] *See* https://www.sec.gov/Archives/edgar/data/882235/000119312512074448/d258295dex211.htm (last accessed Dec. 27, 2022).

37. Defendant acquired, collected, and stored Representative Plaintiffs' and Class Members' PII/PHI and/or financial information to facilitate the healthcare services Representative Plaintiffs and Class Members requested or received.

38. Defendant has or has had approximately two million customers, according to its website.[6]

39. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged here are currently unknown to Representative Plaintiffs. Representative Plaintiffs will seek leave of court to amend this Complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

COMMON FACTUAL ALLEGATIONS

The Data Breach

40. On September 26, 2021, Defendant "identified unusual activity on certain systems within its network."[7]

41. Defendant then "launched an investigation, including working with outside cybersecurity experts to determine the source of the activity and potential impact on Lincare's network."[8]

[6] https://www.lincare.com/en/why-lincare (last accessed December 20, 2022).
[7] https://www.lincare.com/-/media/project/lincare/files/security_notice.pdf.
[8] *Id.*

42. Although Defendant did not become aware of the Data Breach until September 26, 2021, Defendant's "investigation confirmed that certain systems may have first been accessed on September 10, 2021," more than two weeks beforehand.[9]

43. Although Defendant became aware of the Data Breach on September 26, 2021, the "unauthorized access was [not] blocked [until] September 29, 2021," three days after the reported discovery.[10]

44. Defendant concluded, that in the course of the Data Breach, one or more unauthorized third parties accessed Plaintiffs' and Class Members' sensitive data, including but not limited to, social security numbers, names, dates of birth, and medical information, such as medical treatments, provider names, dates of service, diagnosis/procedure, account or record numbers, health insurance information, and prescription information.

45. Upon information and belief, the unauthorized third-party cybercriminals gained access to Representative Plaintiffs' and Class Members' PII/PHI and financial information with the intent of engaging in misuse of the PII/PHI and financial information, including marketing and selling Representative Plaintiffs' and Class Members' PII/PHI.

46. While Defendant has yet to report the total number of affected

[9] *Id.*
[10] *Id.*

individuals to the Department of Health and Human Services (as of August 10, 2022),[11] according to separate and sporadic reports made to the Montana,[12] New Hampshire,[13] Texas,[14] Washington,[15] and Massachusetts[16] Attorneys General, the Data Breach compromised the PII/PHI of at least 172,052 individuals. For example, Defendant reported to the Texas Attorney General's office that the names, Social Security numbers, driver's license numbers, and medical/health insurance information of 115,394 Texans had been compromised. [17]

Defendant's Failed Response to the Breach

47. Time is of the essence when highly sensitive PII/PHI is subject to unauthorized access and/or acquisition. The disclosed, accessed, and/or acquired PII/PHI of Representative Plaintiffs and Class Members is likely available on the Dark Web. Hackers can access and then offer for sale the unencrypted, unredacted PII/PHI to criminals. Representative Plaintiffs and Class Members are now subject

[11] Despite Defendant's reporting requirements, the HHS Office of Civil Rights Breach Portal still states that "500 individuals" were impacted, a number that usually serves as a placeholder until the entity determines the total number. *See* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Aug. 10, 2022).
[12] https://dojmt.gov/consumer/databreach/ (last visited Aug. 10, 2022).
[13] https://www.doj.nh.gov/consumer/security-breaches/documents/lincare-holdings-20220613.pdf (last visited Aug. 10, 2022).
[14] https://oagtx.force.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last visited Aug. 10, 2022).
[15] https://agportal-s3bucket.s3.amazonaws.com/databreach/BreachM13355.pdf. (last visited Aug. 10, 2022).
[16] https://www.mass.gov/doc/assigned-data-beach-number-25976-lincare-holdings-inc/download. (last visited Aug. 10, 2022).
[17] *See, e.g.* https://oagtx.force.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last visited Aug. 10, 2022).

to the present and continuing risk of fraud, identity theft, and misuse resulting from the possible publication of their PII/PHI, especially their Social Security numbers and sensitive medical information, onto the Dark Web. Representative Plaintiffs and Class Members now face a lifetime risk of identity theft, which is heightened here by unauthorized access, disclosure, and/or activity by cybercriminals on computer systems containing hundreds of thousands of Social Security numbers and/or specific, sensitive medical information.

48. Despite this understanding, Defendant did not begin informing affected individuals, including Representative Plaintiffs and Class Members, about the Data Breach for months. In fact, it was not until nine months after it claims to have discovered the Data Breach that Defendant began sending the Notice to persons whose PII/PHI was compromised in the Data Breach. The Notice provided only basic details of the Data Breach and Defendant's recommended next steps.

49. Representative Plaintiffs and the Class Members remain, even today, in the dark regarding what particular data was stolen, the particular malware used, and what steps are being taken, if any, to secure their PII/PHI and financial information going forward. Representative Plaintiffs and Class Members are left to speculate as to the full impact of the Data Breach and how exactly Defendant intends to enhance its information security systems and monitoring capabilities so as to prevent further breaches.

50. Representative Plaintiffs' and Class Members' PII/PHI may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII/PHI for targeted marketing without the approval of Representative Plaintiffs or Class Members. Either way, unauthorized individuals can now easily access the PII/PHI of Representative Plaintiffs and Class Members.

51. Moreover, Defendant put the burden squarely on Representative Plaintiffs and Class Members to enroll in the inadequate monitoring services, among other steps Plaintiffs and Class Members must take to protect themselves.

52. Following the Breach and recognizing that each Class Member is now subject to the present and continuing risk of identity theft and fraud, Defendant encouraged Plaintiffs and Class Members "to remain vigilant against incidents of identity theft and fraud, to review all claims information from your health insurance provider, and to monitor your credit reports and financial statements for suspicious activity."[18]

53. Defendant also encouraged Plaintiffs and Class Members to "report any suspicious activity to the credit bureaus at the numbers listed below in this letter."[19] Defendant further encouraged Plaintiffs and Class Members to "review the information we are enclosing in this letter about steps you can take to help protect

[18] https://www.doj.nh.gov/consumer/security-breaches/documents/lincare-holdings-20220613.pdf at 4.
[19] *Id.*

your personal information *as you deem appropriate*."[20]

54. Defendant also informed Plaintiffs and Class Members that they could "FREEZE YOUR CREDIT FILE," "PLACE FRAUD ALERTS ON YOUR CREDIT FILE," "REMAIN VIGILANT: REVIEW YOUR ACCOUNT STATEMENTS, & REPORT FRAUD," "ORDER YOUR FREE ANNUAL CREDIT REPORTS," and "OBTAIN INFORMATION ABOUT PREVENTING IDENTITY THEFT FROM FTC / STATE ATTORNEY GENERAL."[21]

55. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.5% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.[22]

56. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week;[23] leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'"[24] Usually, this time can be spent

---

[20] *Id.*
[21] *Id. at 5.*
[22] U.S. BUREAU OF LABOR STATISTICS, Wage Worker Survey, *available at* https://www.bls.gov/opub/reports/minimum-wage/2020/home.htm#:~:text=In%202020%2C%2073.3%20million%20workers,wage%20of%20%247.25%20per%20hour (last visited Dec. 27, 2022); *see also* U.S. BUREAU OF LABOR STATISTICS, *Employment And Average Hourly Earnings By Industry, available at* https://www.bls.gov/charts/employment-situation/employment-and-average-hourly-earnings-by-industry-bubble.htm (last visited Dec. 29, 2022) (finding that on average, private-sector workers make $1,312.80 per 40-hour work week.).
[23] *See* https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html (last visited Dec. 27, 2022).
[24] *Id.*

at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

57. Representative Plaintiffs and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek renumeration for the loss of valuable time as another element of damages.

Defendant's Data Security Failures

58. Despite the prevalence of public announcements of data breaches and data security compromises, Defendant failed to take appropriate steps to protect Plaintiffs' and Class Members' PII/PHI from being compromised.

59. Defendant's Notice demonstrated that Defendant made several data security failures that led to the Data Breach:

a) Defendant failed to properly monitor and log file and system access.[25]

b) Defendant failed to properly monitor and log the ingress and egress of network traffic.[26]

c) Defendant failed to properly monitor and detect suspicious activity and

[25] https://www.lincare.com/-/media/project/lincare/files/security_notice.pdf ("certain systems *may* have first been accessed" and "the incident *may* have resulted in unauthorized access to some patient personal information").
[26] *Id.* ("certain systems *may* have first been accessed" and "the incident *may* have resulted in unauthorized access to some patient personal information").

threats.[27]

d) Defendant failed to ensure proper staffing and implement sufficient processes to prevent, quickly detect, and respond to data breaches, security incidents, or intrusions.[28]

e) Defendant failed to properly train its employees as to cybersecurity best practices.

f) Defendant failed to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PII/PHI of Plaintiffs and Class Members.

g) Defendant failed to timely and accurately disclose that Plaintiffs' and Class Members' PII/PHI had been improperly acquired or accessed.

h) Defendant knowingly disregarded standard information security principles, despite obvious risks, by allowing unmonitored and unrestricted access to unsecured PII/PHI.

i) Defendant failed to provide adequate supervision and oversight of the PII/PHI with which it was and is entrusted, in spite of the known risk and

[27] *Id.* (Although Defendant first became aware of the Data Breach on September 26, 2021, Defendant's "investigation confirmed that certain systems may have first been accessed on September 10, 2021," more than two weeks before).

[28] *Id.* (The investigation "required customized protocols and programming in order to analyze the data and identify key information," and "a manual review of the data." And although Defendant became aware of the Data Breach on September 26, 2021, the "unauthorized access was [not] blocked [until] September 29, 2021," three days later.).

foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII/PHI of Plaintiffs and Class Members, misuse the PII/PHI and potentially disclose it to others without consent.

j) Defendant failed to properly encrypt Plaintiffs' and Class Members' PII/PHI and monitor user behavior and activity to identify possible threats.[29]

60. Further, this is not Defendant's first breach of cybersecurity entrusted to it. For example, on February 10, 2017, Lincare sent notice of a "phishing attack" to current and former Lincare employees, notifying them that their personally identifiable information may have been compromised.[30]

61. Thus, Defendant was on notice that the information within its systems was highly sought-after and valuable to cyber attackers who would attempt to use that information for nefarious purposes.

Representative Plaintiff's B.B.'s Experience

62. Plaintiff has received services or products from Lincare for several years.

63. Shortly after and as a result of the Data Breach, Plaintiff B.B.

[29] *Id.* ("certain systems *may* have first been accessed" and "the incident *may* have resulted in unauthorized access to some patient personal information").
[30] Theresa Flaherty, *Lincare Settles Employee Data Breach Claims*, HMENews (May 17, 2018), *available at* https://www.hmenews.com/article/lincare-settles-employee-data-breach-claims.

experienced an increase in spam and suspicious phone calls, texts, targeted health advertisements, and emails.

64. On or about June 23, 2022, Plaintiff B.B. received a letter from Defendant, dated June 21, 2022, notifying her that her PII/PHI had been improperly accessed and/or obtained by unauthorized third parties in the Data Breach.

65. As a result of the Data Breach and at the recommendation of Defendant, Plaintiff B.B. made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing her online account passwords, and monitoring her credit information as suggested by Defendant.

66. Plaintiff B.B. has spent approximately 15 hours responding to the Data Breach and will continue to spend valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation.

67. Plaintiff B.B. suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced anxiety and increased concerns for the loss of her privacy, as well as anxiety over the impact of cybercriminals accessing and using her PII/PHI and/or financial information.

68. Plaintiff B.B. is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from her PII/PHI and financial information, in combination with her name, being placed in the hands of unauthorized third

parties/criminals. This injury was worsened by Defendant's nine-month long delay in informing Plaintiffs and Class Members about the Data Breach.

69. Plaintiff B.B. has a continuing interest in ensuring that her PII/PHI, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Representative Plaintiff Martha Chang's Experience

70. Plaintiff Chang has received services and products from Lincare for more than ten years.

71. Shortly after and as a result of the Data Breach, Plaintiff Chang experienced an increase in spam and suspicious phone calls, texts, targeted health advertisements, and emails.

72. On or about June 19, 2022, Plaintiff Chang received a letter from Defendant, dated June 17, 2022, notifying her that her PII/PHI had been improperly accessed and/or obtained by unauthorized third parties in the Data Breach.

73. As a result of the Data Breach and at the recommendation of Defendant, Plaintiff Chang made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing her online account passwords, and monitoring her credit information as suggested by Defendant.

74. Plaintiff Chang has spent approximately 10 hours responding to the

Data Breach and will continue to spend valuable time she/he otherwise would have spent on other activities, including but not limited to work and/or recreation.

75. Plaintiff Chang suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced anxiety, sleep disruption, and increased concerns for the loss of her privacy, as well as anxiety over the impact of cybercriminals accessing and using her PII/PHI and/or financial information.

76. Plaintiff Chang is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from her PII/PHI and financial information, in combination with her name, being placed in the hands of unauthorized third parties/criminals. This injury was worsened by Defendant's nine-month long delay in informing Plaintiffs and Class Members about the Data Breach.

77. Plaintiff Chang has a continuing interest in ensuring that her PII/PHI, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Representative Plaintiff Fudge's Experience

78. On or about December 2020, Plaintiff Fudge received services or products from Lincare.

79. Shortly after and as a result of the Data Breach, Plaintiff Fudge experienced an increase in spam and suspicious phone calls, texts, targeted health

advertisements, and emails.

80. On or about June 10, 2022, Plaintiff Fudge received a letter from Defendant, dated June 6, 2022, notifying him that his PII/PHI had been improperly accessed and/or obtained by unauthorized third parties in the Data Breach.

81. As a result of the Data Breach and at the recommendation of Defendant, Plaintiff Fudge made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing his online account passwords, and monitoring her credit information as suggested by Defendant.

82. Plaintiff Fudge has spent approximately 10 hours responding to the Data Breach and will continue to spend valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation.

83. Plaintiff Fudge suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced anxiety, difficulty sleeping, and increased concerns for the loss of his privacy, as well as anxiety over the impact of cybercriminals accessing and using his PII/PHI and/or financial information.

84. Plaintiff Fudge is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his PII/PHI and financial information, in combination with his name, being placed in the hands of unauthorized third

parties/criminals. This injury was worsened by Defendant's nine-month long delay in informing Plaintiffs and Class Members about the Data Breach.

85. Plaintiff Fudge has a continuing interest in ensuring that his PII/PHI, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Representative Plaintiff Victor Juarez's Experience

86. Plaintiff Juarez first received Lincare's services and products in or around April of 2020.

87. Shortly after and as a result of the Data Breach, Plaintiff Juarez discovered that his identity was stolen. More specifically, someone used his information to fraudulently file for unemployment benefits and open an unemployment account.

88. Shortly after and as a result of the Data Breach, Plaintiff Juarez also experienced an increase in spam and suspicious phone calls, texts, targeted health advertisements, and emails.

89. On or about June 24, 2022, Plaintiff Juarez received a letter from Defendant, dated June 21, 2022, notifying him that his PII/PHI had been improperly accessed and/or obtained by unauthorized third parties in the Data Breach.

90. Plaintiff Juarez had never been a victim of a data breach prior to Defendant's Breach.

91. Plaintiff Juarez never experienced identity theft or targeted spam and phishing attempts prior to the data breach.

92. As a result of the Data Breach and at the recommendation of Defendant, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing his online account passwords, and monitoring his credit information as suggested by Defendant.

93. Plaintiff Juarez has spent approximately 50 hours responding to the Data Breach and will continue to spend valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation.

94. Plaintiff Juarez suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced anxiety and increased concerns for the loss of his privacy, as well as anxiety over the impact of cybercriminals accessing and using his PII/PHI and/or financial information.

95. Plaintiff Juarez is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his PII/PHI and financial information, in combination with his name, being placed in the hands of unauthorized third parties/criminals. This injury was worsened by Defendant's nine-month long delay in informing Plaintiffs and Class Members about the Data Breach.

96. Plaintiff Juarez has a continuing interest in ensuring that his PII/PHI,

which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Representative Plaintiff Merrell's Experience

97. On or about 2001, Plaintiff Merrell began receiving services or products from Lincare.

98. Approximately six months after and as a result of the Data Breach, Plaintiff Merrell received an alert from Experian credit monitoring that her PII/PHI had been found on the dark web.

99. Shortly after and as a result of the Data Breach, Plaintiff Merrell experienced an increase in spam and suspicious phone calls, texts, targeted health advertisements, and emails.

100. On or about June 18, 2022, 2022, Plaintiff Merrell received a letter from Defendant, dated June 16, 2022, notifying her that her PII/PHI had been improperly accessed and/or obtained by unauthorized third parties in the Data Breach.

101. Plaintiff Merrell had never been a victim of a data breach prior to Defendant's Breach.

102. As a result of the Data Breach and at the recommendation of Defendant, Plaintiff Merrell made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing her online account passwords, and

monitoring her credit information as suggested by Defendant.

103. Plaintiff Merrell has spent approximately two hours responding to the Data Breach and will continue to spend valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation.

104. Plaintiff Merrell suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced anxiety and increased concerns for the loss of her privacy, as well as anxiety over the impact of cybercriminals accessing and using her PII/PHI and/or financial information.

105. Plaintiff Merrell is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from her PII/PHI and financial information, in combination with her name, being placed in the hands of unauthorized third parties/criminals. This injury was worsened by Defendant's nine-month long delay in informing Plaintiffs and Class Members about the Data Breach.

106. Plaintiff Merrell has a continuing interest in ensuring that her PII/PHI, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Representative Plaintiff Miller's Experience

107. On or about October 2020, Plaintiff Miller received services or products from Lincare.

108. Shortly after and as a result of the Data Breach, Plaintiff Miller

discovered that an unknown criminal attempted to open several credit cards in his name.

109. Shortly after and as a result of the Data Breach, Plaintiff Miller experienced an increase in spam and suspicious phone calls, texts, targeted health advertisements, and emails.

110. On or about October 2022, Plaintiff Miller received a letter from Defendant, notifying him that his PII/PHI had been improperly accessed and/or obtained by unauthorized third parties in the Data Breach.

111. Plaintiff Miller had never been a victim of a data breach prior to Defendant's Breach.

112. As a result of the Data Breach and at the recommendation of Defendant, Plaintiff Miller made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing her online account passwords, and monitoring her credit information as suggested by Defendant.

113. Plaintiff Miller has spent approximately six hours responding to the Data Breach and will continue to spend valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation.

114. Plaintiff Miller suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced anxiety and

increased concerns for the loss of her/his privacy, as well as anxiety over the impact of cybercriminals accessing and using her/his PII/PHI and/or financial information.

115. Plaintiff Miller is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his PII/PHI and financial information, in combination with his name, being placed in the hands of unauthorized third parties/criminals. This injury was worsened by Defendant's ten-month long delay in informing Plaintiff and Class Members about the Data Breach.

116. Plaintiff Miller has a continuing interest in ensuring that his PII/PHI, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Representative Plaintiff Torres's Experience

117. Beginning in approximately 2007 or 2008 and continuing until sometime in 2022, Plaintiff Torres received services or products from Lincare.

118. Shortly after and as a result of the Data Breach, Plaintiff Torres discovered fraudulent charges and activity with respect to her banking accounts. This includes the unauthorized withdrawals from one account in the amount of approximately $10,000, documented by a police report one month after notification of the Data Breach. She also suffered additional fraudulent account activity resulting in the suspension of a bank account for which she had never opened, multiple attempts to open and change the banking information for her direct deposits to yet

another bank that she did not bank with, and fraudulent PayPal charges in an amount of $695, including fraudulent charges for computer software and a refrigerator.

119. Shortly after and as a result of the Data Breach, Plaintiff Torres experienced an increase in spam and suspicious phone calls, texts, targeted health advertisements, and emails. Most recently, on or about December 27, 2022, Plaintiff Torres received a letter dated December 16, 2022 from One Main Financial denying her approval of a loan application purported to be made by her for the purchase of a motor vehicle on December 12, 2022 – an application she did not submit and a vehicle she knew nothing about.

120. In approximately mid-June of 2022, Plaintiff Torres received a letter from Defendant, dated June 6, 2022, notifying her that her PII/PHI had been improperly accessed and/or obtained by unauthorized third parties in the Data Breach.

121. As a result of the Data Breach and at the recommendation of Defendant, Plaintiff Torres made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing her online account passwords, and monitoring her credit information as suggested by Defendant.

122. Since receiving notification of the breach, Plaintiff Torres has spent approximately 10 hours responding to the Data Breach and will continue to spend

valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation.

123. Plaintiff Torres suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced anxiety and increased concerns for the loss of her privacy, as well as anxiety over the impact of cybercriminals accessing and using her PII/PHI and/or financial information.

124. Plaintiff Torres is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from her PII/PHI and financial information, in combination with her name, being placed in the hands of unauthorized third parties/criminals. This injury was worsened by Defendant's more than eight-month long delay in informing Plaintiffs and Class Members about the Data Breach.

125. Plaintiff Torres has a continuing interest in ensuring that her PII/PHI, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Defendant Collected/Stored Class Members' PII/PHI and Financial Information

126. Defendant acquired, collected, and stored, and assured reasonable security over, Representative Plaintiffs' and Class Members' PII/PHI and financial information.

127. As a condition of its relationships with Representative Plaintiffs and

Class Members, Defendant required that Representative Plaintiffs and Class Members entrust Defendant with highly sensitive and confidential PII/PHI and financial information. Defendant, in turn, stored that information on its system that was ultimately affected by the Data Breach.

128. Representative Plaintiffs and Class Members were required to provide their PII/PHI and financial information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

129. By obtaining, collecting, and storing Representative Plaintiffs' and Class Members' PII/PHI and financial information, Defendant assumed legal and equitable duties and knew, or should have known, that they were thereafter responsible for protecting Representative Plaintiffs' and Class Members' PII/PHI and financial information from unauthorized disclosure.

130. Representative Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII/PHI and financial information. Representative Plaintiffs and Class Members relied on Defendant to keep their PII/PHI and financial information confidential and securely maintained, to use this information for business and healthcare purposes only, and to make only authorized disclosures of this information.

131. Defendant could have prevented the Data Breach by properly

securing and encrypting and/or more securely encrypting its servers generally, as well as Representative Plaintiffs' and Class Members' PII/PHI and financial information.

132. Defendant's negligence in safeguarding Representative Plaintiffs' and Class Members' PII/PHI and financial information is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

133. The healthcare industry in particular has experienced a large number of high-profile cyberattacks even in just the short period preceding the filing of this Complaint and cyberattacks, generally, have become increasingly more common. More healthcare data breaches were reported in 2020 than in any other year, showing a 25% increase.[31] Additionally, according to the HIPAA Journal, the largest healthcare data breaches have been reported beginning in April 2021.[32]

134. This trend continues in 2022, and healthcare breaches continue to increase in record numbers.[33] Thus, Defendant was on further notice regarding the increased risks of inadequate cybersecurity. In February 2022, the cybersecurity arm of the U.S. Department of Health and Human Services ("HHS") issued a warning to

[31] *2020 Healthcare Data Breach Report,* https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/ (last accessed Dec. 27, 2022).
[32] *April 2021 Healthcare Data Breach Report,* https://www.hipaajournal.com/april-2021-healthcare-data-breach-report/ (last accessed Dec. 27, 2022).
[33] *June 2022 Healthcare Data Breach Report,* https://www.hipaajournal.com/june-2022-healthcare-data-breach-report/ (last accessed Dec. 27, 2022).

hospitals and healthcare systems about a dramatic rise in cyberattacks, including ransomware attacks, urging facilities to shore up their cyber defenses.[34] Indeed, just days before, HHS's cybersecurity arm issued yet another warning about increased cyberattacks that urged vigilance with respect to data security.[35]

135. In the context of data breaches, healthcare is "by far the most affected industry sector."[36] Further, cybersecurity breaches in the healthcare industry are particularly devastating, given the frequency of such breaches and the fact that healthcare providers maintain highly sensitive and detailed PII.[37]

136. A Tenable study analyzing publicly disclosed healthcare sector breaches from January 2020 to February 2021 reported that "records were confirmed to have been exposed in *nearly 93% of the breaches*."[38]

137. This is such a breach of cybersecurity where highly detailed PII/PHI records maintained, collected, and stored by a healthcare entity were accessed and/or

---

[34] Rebecca Pifer, *Tenet says 'cybersecurity incident' disrupted hospital operations*, HEALTHCAREDIVE (Apr. 26, 2022), https://www.healthcaredive.com/news/tenet-says-cybersecurity-incident-disrupted-hospital-operations/622692/ (last accessed Dec. 27, 2022).

[35] *Id.* (HHS warned healthcare providers about the increased potential for attacks by a ransomware group called Hive, "[c]alling it one of the 'most active ransomware operators in the cybercriminal ecosystem,' the agency said reports have linked Hive to attacks on 355 companies within 100 days of its launch last June — nearly three a day.").

[36] Tenable Security Response Team, *Healthcare Security*, TENABLE (Mar. 10, 2021), https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches (last accessed Dec. 27, 2022).

[37] *See id.*

[38] Tenable Security Response Team, *Healthcare Security*, TENABLE (Mar. 10, 2021), https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches (last accessed Dec. 27, 2022).

acquired by a cybercriminal.

138. Due to the high-profile nature of these breaches, and other breaches of its kind, and Defendant's own 2017 breach, Defendant was and/or certainly should have been on notice and aware of such attacks occurring in the healthcare industry and, therefore, should have assumed and adequately performed the duty of preparing for such an imminent attack. This is especially true given that Defendant is a large, sophisticated operation with the resources to put adequate data security protocols in place.

139. Yet, despite the prevalence of public announcements of data breach and data security compromises, and Defendant's own previous breach of protected information, Defendant failed to take appropriate steps to protect Representative Plaintiffs' and Class Members' PII/PHI and financial information from being compromised.

140. Further, as a healthcare provider, Defendant was on notice that companies in the healthcare industry are targets for data breaches.

Defendant Had an Obligation to Protect the PII/PHI

141. Defendant had and continues to have obligations created by HIPAA, the Alabama Data Breach Notification Act of 2018,[39] reasonable industry standards, common law, state statutory law, and its own assurances and representations to

[39] Specifically, Ala. Code § 8-38-3 and Ala. Code § 8-38-5.

keep Representative Plaintiffs' and Class Members' PII/PHI confidential and to protect such PII/PHI from unauthorized access.

142. Defendant's failure to adequately secure Representative Plaintiffs' and Class Members' sensitive data breaches the duties it owes Representative Plaintiffs and Class Members under statutory and common law. As a covered entity, Defendant has a statutory duty under HIPAA and other federal and state statutes to safeguard Representative Plaintiffs' and Class Members' data.

143. Moreover, Representative Plaintiffs and Class Members surrendered their highly sensitive personal data to Defendant under the implied condition that Defendant would keep it private and secure. Accordingly, Defendant also has an implied duty to safeguard their data, independent of any statute.

Defendant's Conduct Violates Federal Law, Including the Rules and Regulations of HIPAA and HITECH

144. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, et seq. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI like the data Defendant left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

145. Defendant is a covered entity pursuant to HIPAA. *See* 45 C.F.R. §

160.102. Defendant must therefore comply with the HIPAA Privacy Rule and Security Rule. See 45 C.F.R. Part 160 and Part 164, Subparts A through E.

146. Defendant is a covered entity pursuant to the Health Information Technology Act ("HITECH").[40] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

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

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

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

150. HIPAA requires Defendant to "comply with the applicable standards,

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

implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

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

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

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

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

c) Protect Against reasonably anticipated uses or disclosures of such information that are not permitted; and

d) Ensure compliance by its workforce.

153. HIPAA also requires Defendant to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information" under 45 C.F.R. § 164.306(e), and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

154. Moreover, the HIPAA Breach Notification Rule, 45 C.F.R. §§

164.400-414, requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

155. Representative Plaintiffs' and Class Members' Personal and Medical Information, including their PII/PHI, is "protected health information" as defined by 45 CFR § 160.103.

156. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

157. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

158. Representative Plaintiffs' and Class Members' personal and medical information, including their PII/PHI, is "unsecured protected health information" as defined by 45 CFR § 164.402.

159. Representative Plaintiffs' and Class Members' unsecured protected health information has been acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

160. Representative Plaintiffs' and Class Members' unsecured protected health information acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

161. Representative Plaintiffs' and Class Members' unsecured protected health information that was acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

162. Representative Plaintiffs' and Class Members' unsecured protected health information was viewed by unauthorized persons in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

163. After receiving notice that they were victims of a data breach that required the filing of a Breach Report in accordance with 45 CFR § 164.408(a), it is reasonable for recipients of that notice, including Representative Plaintiffs and Class Members in this case, to believe that future harm (including identity theft) is real and imminent, and to take steps to mitigate that risk of future harm.

164. The Data Breach could have been prevented if Defendant implemented HIPAA mandated, industry standard policies and procedures for securely disposing of PHI when it was no longer necessary and/or had honored its obligations to its

patients.

165. It can be inferred from Defendant's Data Breach that Defendant either failed to implement, or inadequately implemented, information security policies or procedures in place to protect Representative Plaintiffs' and Class Members' PII/PHI.

166. Defendant's security failures include, but are not limited to:

a. Failing to maintain an adequate data security system and safeguards to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data, including identifying internal and external risks of a security breach;

c. Failing to ensure the confidentiality and integrity of electronic protected health information Defendant creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR

164.308(a)(1);

f. Failing 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 CFR 164.308(a)(6)(ii);

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

h. Failing 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 CFR 164.306(a)(3);

i. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce in violation of 45 CFR 164.306(a)(94);

j. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq*.; and

k. Retaining information past a recognized purpose and not deleting it.

167. Upon information and belief, prior to the Breach, Defendant was aware of its security failures but failed to correct them or to disclose them to the public,

including Plaintiffs and Class Members.

168. The implementation of proper encryption, logging, detection, training, and monitoring protocols requires affirmative acts. Accordingly, Defendant knew or should have known that it did not make such actions and failed to implement adequate data security practices.

169. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required Defendant to provide notice of the Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

170. Because Defendant has failed to comply with industry standards, while monetary relief may cure some of Representative Plaintiffs and Class Members' injuries, injunctive relief is necessary to ensure Defendant's approach to information security is adequate and appropriate. Defendant still maintains the PII/PHI of Representative Plaintiffs and Class Members; and without the supervision of the Court via injunctive relief, Representative Plaintiffs' and Class Members' PII/PHI remains at risk of subsequent Data Breaches.

171. Defendant was also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data

security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g.*, *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

172. In addition to its obligations under federal and state laws, Defendant owed a duty to Representative Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII/PHI and financial information in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Representative Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII/PHI and financial information of Representative Plaintiffs and Class Members.

173. Defendant owed a duty to Representative Plaintiffs and Class Members to design, maintain, and test its computer systems, servers and networks to ensure that the PII/PHI and financial information in its possession was adequately secured and protected.

174. Defendant owed a duty to Representative Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect the PII/PHI and financial information in its possession, including not sharing

information with other entities who maintained sub-standard data security systems.

175. Defendant owed a duty to Representative Plaintiffs and Class Members to implement processes that would immediately detect a breach on its data security systems in a timely manner.

176. Defendant owed a duty to Representative Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

177. Defendant owed a duty to Representative Plaintiffs and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII/PHI and/or financial information from theft because such an inadequacy would be a material fact in the decision to entrust this PII/PHI and/or financial information to Defendant.

178. Defendant owed a duty of care to Representative Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

179. Defendant owed a duty to Representative Plaintiffs and Class Members to encrypt and/or more reliably encrypt Representative Plaintiffs' and Class Members' PII/PHI and financial information and monitor user behavior and activity in order to identity possible threats.

180. Defendant owed a duty to Representative Plaintiffs and Class Members to mitigate the harm suffered by the Representative Plaintiffs' and Class Members'

PII/PHI as a result of the Data Breach.

Value of the Relevant Sensitive Information

181. While the greater efficiency of electronic health records translates to cost savings for providers, it also comes with the risk of privacy breaches. These electronic health records contain a plethora of sensitive information (e.g., patient data, patient diagnosis, lab results, RX's, treatment plans) that is valuable to cyber criminals. One patient's complete record can be sold for hundreds of dollars on the dark web. As such, PII/PHI and financial information are valuable commodities for which a "cyber black market" exists in which criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on a number of underground internet websites. Unsurprisingly, the healthcare industry is at high risk for and acutely affected by cyberattacks.

182. The high value of PII/PHI and financial information to criminals is further evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[41] Experian reports that a stolen credit or debit card

[41] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Dec. 27, 2022).

number can sell for $5 to $110 on the dark web.[42] Criminals can also purchase access to entire company data breaches from $999 to $4,995.[43]

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

184. These criminal activities have and will result in devastating financial and personal losses to Representative Plaintiffs and Class Members. For example, it is believed that certain PII compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma. Such fraud will be an omnipresent threat for Representative Plaintiffs and Class Members for the rest of their lives. They will

---

[42] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Dec. 27, 2022).

[43] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Dec. 27, 2022, 2022).

[44] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133 (last accessed Dec. 27, 2022).

[45] https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/ (last accessed Dec. 27, 2022).

[46] https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches (last accessed Dec. 27, 2022).

need to remain constantly vigilant.

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

186. Identity thieves can use PII/PHI and financial information, such as that of Representative Plaintiffs and Class Members which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

187. The ramifications of Defendant's failure to keep secure Representative Plaintiffs' and Class Members' PII/PHI and financial information are long lasting and severe. Once PII/PHI and financial information is stolen, particularly

identification numbers, fraudulent use of that information and damage to victims may continue for years. Indeed, the PII/PHI and/or financial information of Representative Plaintiffs and Class Members was taken by hackers to engage in identity theft or to sell it to other criminals who will purchase the PII/PHI and/or financial information for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

188. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII/PHI and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[47]

189. The harm to Representative Plaintiffs and Class Members is especially acute given the nature of the leaked data. Medical identity theft is one of the most common, most expensive, and most difficult-to-prevent forms of identity theft. According to Kaiser Health News, "medical- related identity theft accounted for 43

[47] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last accessed Dec. 27, 2022).

percent of all identity thefts reported in the United States in 2013," which is more than identity thefts involving banking and finance, the government and the military, or education.[48]

190. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[49]

191. If cyber criminals manage to access financial information, health insurance information and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Defendant may have exposed Representative Plaintiffs and Class Members.

192. A study by Experian found that the average total cost of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[50] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third saw

[48] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, KAISER HEALTH NEWS (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft/ (last accessed Dec. 27, 2022).
[49] *Id.*
[50] *See* Elinor Mills, *Study: Medical Identity Theft is Costly for Victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed Dec. 27, 2022).

their insurance premiums rise, and forty percent were never able to resolve their identity theft at all.[51]

193. Data breaches are preventable.[52] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[53] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised."[54]

194. Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[55]

195. Defendant was, or should have been, fully aware of the unique type and the significant volume of data stored on and/or shared on its system, amounting to

---

[51] *Id.*; *see also Healthcare Data Breach: What to Know About them and What to Do After One*, EXPERIAN, *available at* https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last accessed Dec. 27, 2022).
[52] Lucy L. Thompson, *Despite the Alarming Trends, Data Breaches Are Preventable*, *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012)
[53] *Id.* at 17.
[54] *Id.* at 28.
[55] *Id.*

more than 172,000 individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

196. Following the breach and recognizing that Representative Plaintiffs, along with each and every Class Member, are now subject to the present and continuing risk of identity theft and fraud, Defendant offered Representative Plaintiffs and Class Members only twelve months of credit monitoring, fraud consultation, and identity theft restoration services through a single provider, Kroll. The offered services are insufficient to protect Representative Plaintiffs and Class Members from the lifelong implications of having their most private PII/PHI accessed, acquired, exfiltrated, and/or published onto the internet. As another element of damages, Representative Plaintiffs and Class Members seek a sum of money sufficient to provide to Representative Plaintiffs and Class Members identity theft protective services for their respective lifetimes.

197. The injuries to Representative Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII/PHI of Representative Plaintiffs and Class Members.

198. Here, Defendant knew of the importance of safeguarding PII/PHI and financial information and of the foreseeable consequences that would occur if

Representative Plaintiffs' and Class Members' PII/PHI and financial information was stolen, including the significant costs that would be placed on Representative Plaintiffs and Class Members as a result of a breach of this magnitude. As detailed above, Defendant is a large, sophisticated organization with the resources to deploy robust cybersecurity protocols. It knew, or should have known, that the development and use of such protocols were necessary to fulfill its statutory and common law duties to Representative Plaintiffs and Class Members. Its failure to do so is, therefore, intentional, willful, reckless, and/or grossly negligent.

199. Defendant disregarded the rights of Representative Plaintiffs and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Representative Plaintiffs' and Class Members' PII/PHI and/or financial information; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Representative Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

CLASS ACTION ALLEGATIONS

200. Representative Plaintiffs brings this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of himself and the following class/subclass (collectively, the "Class"):

Nationwide Class:
"All individuals residing in the United States of America whose PII/PHI was stored by Defendant and exposed to unauthorized third-parties as a result of the data breach occurring between September 10, 2021 and September 29, 2021."

Alabama Subclass:
"All individuals residing in the State of Alabama whose PII/PHI was stored by Defendant and exposed to unauthorized third-parties as a result of the data breach occurring between September 10, 2021 and September 29, 2021."

California Subclass:
"All individuals residing in the State of California whose PII/PHI was stored by Defendant and exposed to unauthorized third-parties as a result of the data breach occurring between September 10, 2021 and September 29, 2021."

Georgia Subclass:
"All individuals residing in the State of Georgia whose PII/PHI was stored by Defendant and exposed to unauthorized third-parties as a result of the data breach occurring between September 10, 2021 and September 29, 2021."

Missouri Subclass:
"All individuals residing in the State of Missouri whose PII/PHI was stored by Defendant and exposed to unauthorized third-parties as a result of the data breach occurring between September 10, 2021 and September 29, 2021."

New York Subclass:
"All individuals residing in the State of New York whose PII/PHI was stored by Defendant and exposed to unauthorized third-parties as a result of the data breach occurring between September 10, 2021 and September 29, 2021."

> **North Carolina Subclass:**
> "All individuals residing in the State of North Carolina whose PII/PHI was stored by Defendant and exposed to unauthorized third-parties as a result of the data breach occurring between September 10, 2021 and September 29, 2021."

201. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state, or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; members of the jury in this action; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members and staff.

202. Also, in the alternative, Representative Plaintiffs request additional Subclasses as necessary based on the types of PII/PHI that were compromised.

203. Representative Plaintiffs reserve the right to amend the above definitions or to propose additional subclasses in subsequent pleadings and motions for class certification.

204. This action has been brought and may properly be maintained as a class action under Federal Rule of Civil Procedure Rule 23 because there is a well-defined community of interest in the litigation and membership in the proposed classes is

easily ascertainable.

a) **Numerosity**: A class action is the only available method for the fair and efficient adjudication of this controversy. The members of the Class are so numerous that joinder of all members is impractical, if not impossible. Representative Plaintiffs are informed and believe and, on that basis, allege that the total number of Class Members is in the hundreds of thousands of individuals. Membership in the classes will be determined by analysis of Defendant's records.

b) **Commonality**: Representative Plaintiffs and the Class Members share a community of interests in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including, but not necessarily limited to:

1) Whether Defendant had a legal duty to Representative Plaintiffs and the Class to exercise due care in collecting, storing, using, and/or safeguarding their PII/PHI;

2) Whether Defendant knew or should have known of the susceptibility of its data security systems to a data breach;

3) Whether Defendant's security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;

4) Whether Defendant's failure to implement adequate data security measures allowed the Data Breach to occur;

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

6) Whether Defendant adequately, promptly, and accurately informed Representative Plaintiffs and Class Members that their PII/PHI had been compromised;

7) How and when Defendant actually learned of the Data Breach;

8) Whether Defendant's conduct, including its failure to act,

resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the PII/PHI of Representative Plaintiffs and Class Members;

9) Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

10) Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII/PHI of Representative Plaintiffs and Class Members;

11) Whether Representative Plaintiffs and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or an accounting is/are appropriate as a result of Defendant's wrongful conduct;

12) Whether Representative Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

c) **Typicality**: Representative Plaintiffs' claims are typical of the claims of the Class. Representative Plaintiffs and all members of the Class sustained damages arising out of and caused by Defendant's common course of conduct in violation of law, as alleged herein.

d) **Adequacy of Representation**: Representative Plaintiffs in this class action are an adequate representative of the Class in that Representative Plaintiffs has the same interest in the litigation of this case as the Class Members, are committed to vigorous prosecution of this case and have retained competent counsel who are experienced in conducting litigation of this nature. Representative Plaintiffs are not subject to any individual defenses unique from those conceivably applicable to other Class Members or the classes in its entirety. Representative Plaintiffs anticipate no management difficulties in this litigation.

e) **Superiority of Class Action**: Since the damages suffered by individual Class Members, while not inconsequential, may be relatively small, the expense and burden of individual litigation by each member makes or may make it impractical for members of the Class to seek

> redress individually for the wrongful conduct alleged herein. Should separate actions be brought or be required to be brought, by each individual member of the Class, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants. The prosecution of separate actions would also create a risk of inconsistent rulings which might be dispositive of the interests of other Class Members who are not parties to the adjudications and/or may substantially impede their ability to adequately protect their interests.

205. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class(es) in its/their entirety. Defendant's policies and practices challenged herein apply to and affect Class Members uniformly and Representative Plaintiffs' challenge of these policies and practices hinges on Defendant's conduct with respect to the Class(es) in its/their entirety, not on facts or law applicable only to Representative Plaintiffs.

206. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII/PHI of Class Members, and Defendant may continue to act unlawfully as set forth in this Complaint.

207. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

FIRST CLAIM FOR RELIEF
Negligence
(On behalf of Representative Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Representative Plaintiffs and the State Subclasses)

208. Representative Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 202.

209. At all times herein relevant, Defendant owed Representative Plaintiffs and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PII/PHI and financial information and to use commercially reasonable methods to do so. Defendant took on this obligation upon accepting and storing the PII/PHI and financial information of Representative Plaintiffs and Class Members in its computer systems and on its networks.

210. Among these duties, Defendant was expected:

a) to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII/PHI and financial information in its possession;

b) to protect Representative Plaintiffs' and Class Members' PII/PHI and financial information using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

c) to implement processes to quickly detect the Data Breach and to timely act on warnings about data breaches; and

d) to promptly notify Representative Plaintiffs and Class Members of any data breach, security incident, or intrusion that affected or may have affected its PII/PHI and financial information.

211. Defendant knew that the PII/PHI and financial information was private and confidential and should be protected as private and confidential and, thus, Defendant owed a duty of care not to subject Representative Plaintiffs and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

212. Defendant knew, or should have known, of the risks inherent in collecting and storing PII/PHI and financial information, the vulnerabilities of its data security systems, and the importance of adequate security. Defendant knew about numerous, well-publicized data breaches.

213. Defendant knew, or should have known, that its data systems and networks did not adequately safeguard Representative Plaintiffs' and Class Members' PII/PHI and financial information.

214. Only Defendant was in the position to ensure that its systems and protocols were sufficient to protect the PII/PHI and financial information that Representative Plaintiffs and Class Members had entrusted to it.

215. Defendant breached its duties to Representative Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PII/PHI and financial information of Representative Plaintiffs and Class Members.

216. Because Defendant knew that a breach of its systems could damage hundreds of thousands of individuals, including Representative Plaintiffs and Class Members, Defendant had a duty to adequately protect its data systems and the PII/PHI and financial information contained thereon.

217. Representative Plaintiffs' and Class Members' willingness to entrust Defendant with its PII/PHI and financial information was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to protect its systems and the PII/PHI and financial information they stored on them from attack. Thus, Defendant had a special relationship with Representative Plaintiffs and Class Members.

218. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Representative Plaintiffs' and Class Members' PII/PHI and financial information and promptly notify them about the Data Breach. These "independent duties" are untethered to any contract between Defendant and Representative Plaintiffs and/or the remaining Class Members.

219. Defendant breached its general duty of care to Representative Plaintiffs and Class Members in, but not necessarily limited to, the following ways:

a) by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PII/PHI and financial information of Representative Plaintiffs and Class Members;

b) by failing to timely and accurately disclose that Representative Plaintiffs' and Class Members' PII/PHI and financial information had been improperly acquired or accessed; by failing to adequately protect and safeguard the PII/PHI and financial information

c) by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII/PHI and financial information;

d) by failing to provide adequate supervision and oversight of the PII/PHI and financial information with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII/PHI and financial information of Representative Plaintiffs and Class Members, misuse the PII/PHI and intentionally disclose it to others without consent.

e) by failing to adequately train its employees to not store PII/PHI and financial information longer than absolutely necessary;

f) by failing to consistently enforce security policies aimed at protecting Representative Plaintiffs' and the Class Members' PII/PHI and financial information;

g) by failing to implement processes to quickly detect data breaches, security incidents, or intrusions;

h) by failing to encrypt Representative Plaintiffs' and Class Members' PII/PHI and financial information and monitor user behavior and activity in order to identify possible threats; and,

i) by failing to mitigate the harm suffered by the Representative Plaintiffs and Class members as a result of the Data Breach.

220. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

221. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Representative Plaintiffs and Class Members have suffered

damages and are at imminent risk of additional harms and damages (as alleged above).

222. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the PII/PHI and financial information to Representative Plaintiffs and Class Members so that they could and/or still can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII/PHI and financial information.

223. Defendant breached its duty to notify Representative Plaintiffs and Class Members of the unauthorized access by waiting months after learning of the Data Breach to notify Representative Plaintiffs and Class Members and then by failing and continuing to fail to provide Representative Plaintiffs and Class Members sufficient information regarding the breach. To date, Defendant has not provided sufficient information to Representative Plaintiffs and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Representative Plaintiffs and Class Members.

224. Further, through its failure to provide timely and clear notification of the Data Breach to Representative Plaintiffs and Class Members, Defendant prevented Representative Plaintiffs and Class Members from taking meaningful, proactive steps to secure their PII/PHI and financial information, and to access their medical records and histories.

225. There is a close causal connection between Defendant's failure to implement security measures to protect the PII/PHI and financial information of Representative Plaintiffs and Class Members and the harm suffered, or risk of imminent harm suffered by Representative Plaintiffs and Class Members. Representative Plaintiffs' and Class Members' PII/PHI and financial information was accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII/PHI and financial information by adopting, implementing, and maintaining appropriate security measures.

226. Defendant's wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

227. The damages Representative Plaintiffs and Class Members have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

228. As a direct and proximate result of Defendant's negligence, Representative Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII/PHI and financial information is used; (iii) the compromise, publication, and/or theft of their PII/PHI and financial information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII/PHI and financial

information; (v) lost opportunity costs associated with effort expended and the loss of productivity 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 embarrassment and identity theft; (vi) lost continuity in relation to its healthcare; (vii) the continued risk to its PII/PHI and financial information, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Representative Plaintiffs' and Class Members' PII/PHI and financial information in its continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII/PHI and financial information compromised as a result of the Data Breach for the remainder of the lives of Representative Plaintiffs and Class Members.

229. As a direct and proximate result of Defendant's negligence, Representative Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

230. Additionally, as a direct and proximate result of Defendant's negligence, Representative Plaintiffs and Class Members have suffered and will

suffer the continued risks of exposure of their PII/PHI and financial information, which remain in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII/PHI and financial information in its continued possession.

231. As a direct and proximate result of Defendant's negligence, Representative Plaintiffs and Class Members are entitled to and demand actual, consequential, and nominal damages.

SECOND CLAIM FOR RELIEF
NEGELIGENCE *PER SE*
(On behalf of Representative Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Representative Plaintiffs and the State Subclasses)

232. Representative Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 202.

233. 15 U.S.C. § 45 ("FTC Act" or "Section 5") prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PHI/PII and financial information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

234. Defendant violated the FTC Act by failing to use reasonable measures to protect PII/PHI and financial information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII/PHI and financial information it obtained and stored and the foreseeable consequences of the immense damages that would result to Representative Plaintiffs and Class Members.

235. Representative Plaintiffs and Class Members are among the class of persons that Section 5 of the FTC Act, 15 U.S.C. § 45, was enacted to protect. The harm that occurred as a result of the Data Breach is the type of harm the statute was intended to prevent.

236. Defendant's violation of the FTC Act, 15 U.S.C. §45 constitutes negligence *per se*.

237. HIPAA privacy laws were enacted with the objective of protecting the confidentiality of patients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that-if it were to fall into the wrong hands-could present a risk of harm to the patient's finances or reputation.

238. Representative Plaintiffs and Class Members are within the class of

persons that HIPAA privacy laws and HITECH were intended to protect.

239. The harm that occurred as a result of the Data Breach is the type of harm HIPAA and HITECH privacy laws were intended to guard against.

240. Defendant's violations of HIPAA and HITECH constitute negligence *per se*.

241. Defendant violated the Alabama Data Breach Notification Act of 2018 (Ala. Code § 8-38-3, *et seq*.), causing the Data Breach, a harm that the Alabama Data Breach Notification Act of 2018 was intended to prevent.

242. Representative Plaintiff Fudge and the North Carolina Subclass are within the class of persons that the Alabama Data Breach Notification Act of 2018 was intended to protect.

243. Defendant's violation of the Alabama Data Breach Notification Act of 2018 constitutes negligence *per se.*

244. Defendant violated the North Carolina Unfair and Deceptive Trade Practices Act (N.C. Gen. Stat. § 75-1.1, *et seq*.), causing the Data Breach, a harm that the North Carolina Unfair and Deceptive Trade Practices Act was intended to prevent.

245. Representative Plaintiffs Cottam and Torres and the North Carolina Subclass are within the class of persons that the North Carolina Unfair and Deceptive Trade Practices Act was intended to protect.

246. Defendant's violation of the North Carolina Unfair and Deceptive Trade Practices Act (N.C. Gen. Stat. § 75-1.1, *et seq*.) constitutes negligence *per se.*

247. Defendant violated the California Confidentiality of Medical Information Act (Cal. Civ. Code § 56, *et seq*.), the California Consumer Records Act (Cal. Civ. Code § 1798.82, *et seq*.), and the California Unfair Competition Law (Cal. Bus. & Prof. Code, § 17200, *et seq*.), causing the Data Breach, a harm that these Acts were intended to prevent.

248. Representative Plaintiff Juarez and the California Subclass are within the class of persons that the California Confidentiality of Medical Information Act (Cal. Civ. Code § 56, *et seq*.), the California Consumer Records Act (Cal. Civ. Code § 1798.82, *et seq*.), and the California Unfair Competition Law (Cal. Bus. & Prof. Code, § 17200, *et seq*.) were intended to protect.

249. Defendant's violation of the California Confidentiality of Medical Information Act (Cal. Civ. Code § 56, *et seq*.), the California Consumer Records Act (Cal. Civ. Code § 1798.82, *et seq*.), and the California Unfair Competition Law (Cal. Bus. & Prof. Code, § 17200, *et seq*.) constitutes negligence *per se.*

250. Defendant violated New York General Business Law § 349, causing the Data Breach, a harm that New York General Business Law § 349 was intended to prevent.

251. Representative Plaintiff Miller and the New York Subclass are within

the class of persons that New York General Business Law § 349 was intended to protect.

252. Defendant's violation of New York General Business Law § 349 constitutes negligence *per se.*

253. Defendant violated the Missouri Merchandising Practices Act (Mo. Ann. Stat. § 407.010, *et seq*.), causing the Data Breach, a harm that the Missouri Merchandising Practices Act was intended to prevent.

254. Representative Plaintiff Miller and the Missouri Subclass are within the class of persons that the Missouri Merchandising Practices Act was intended to protect.

255. Defendant's violation of the Missouri Merchandising Practices Act constitutes negligence *per se.*

THIRD CLAIM FOR RELIEF
Breach of Fiduciary Duty
(On behalf of Representative Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Representative Plaintiffs and the State Subclasses)

256. Representative Plaintiffs and Class Members re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 202.

257. A relationship existed between Representative Plaintiffs and the Class Members and Defendant in which Plaintiffs and Class Members put their trust in

Defendant to protect the private information of Plaintiffs and Class Members and Defendant accepted that trust.

258. Representative Plaintiffs and Class Members in reasonable reliance upon Lincare's express and implied promises that it would keep their PII/PHI secure in compliance with the standards that are commonplace in the industry and those required by HIPAA, HITECH, and Section 5 of the FTC Act.

259. Defendant breached the fiduciary duty that it owed to Representative Plaintiffs and Class Members by failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest loyalty, and failing to protect the private information of Representative Plaintiffs and Class Members/

260. Defendant's breach of fiduciary duty was a legal cause of damage to Representative Plaintiffs and Class Members.

261. But for Defendant's breach of fiduciary duty, the damage to Representative Plaintiffs and Class Members would not have occurred.

262. Defendant's breach of fiduciary duty contributed substantially to producing the damage to Representative Plaintiffs and Class Members.

263. As a direct and proximate result of Defendant's breach of fiduciary duty, Representative Plaintiffs and Class Members are entitled to and demand actual, consequential, and nominal damages and injunctive relief.

FOURTH CLAIM FOR RELIEF
Breach of Implied Contract

(On behalf of Representative Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Representative Plaintiffs and the State Subclasses)

264. Representative Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 202.

265. Defendant required Representative Plaintiffs and the Nationwide Class to provide and entrust their PII/PHI and financial information as a condition of obtaining medical care and medical devices from Defendant.

266. Representative Plaintiffs and the Nationwide Class paid money to Defendant in exchange for goods and services, as well as Defendant's promises to protect their protected health information and other PII from unauthorized disclosure.

267. Defendant promised to comply with HIPAA and HITECH standards and to make sure that Representative Plaintiffs' and Class Members' protected health information and other PII would remain protected.

268. Through its course of conduct, Defendant, Representative Plaintiff, and Class Members entered into implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Representative Plaintiffs' and Class Members' PII/PHI and financial information.

269. Defendant required Representative Plaintiffs and Class Members to

provide and entrust their PII/PHI and financial information, including medical information, record or account numbers, names, Social Security numbers, Driver's License numbers, email addresses, and dates of birth.

270. Defendant solicited and invited Representative Plaintiffs and Class Members to provide their PII/PHI and financial information as part of Defendant's regular business practices. Representative Plaintiffs and Class Members accepted Defendant's offers and provided their PII/PHI and financial information to Defendant.

271. As a condition of being direct customers/patients of Defendant, Representative Plaintiffs and Class Members provided and entrusted their PII/PHI and financial information to Defendant. In so doing, Representative Plaintiffs and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such non-public information, to keep such information secure and confidential, and to timely and accurately notify Representative Plaintiffs and Class Members if its data had been breached and compromised or stolen.

272. A meeting of the minds occurred when Representative Plaintiffs and Class Members agreed to, and did, provide its PII/PHI and financial information to Defendant, in exchange for, amongst other things, the protection of its PII/PHI and financial information.

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

274. Defendant breached the implied contracts it made with Representative Plaintiffs and Class Members by failing to safeguard and protect their PII/PHI and financial information and by failing to provide timely and accurate notice to them that their PII/PHI and financial information was compromised as a result of the Data Breach.

275. As a condition of obtaining medical care and/or devices from Defendant, Representative Plaintiffs and the Nationwide Class provided and entrusted their personal information. In so doing, Representative Plaintiffs and the Nationwide Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Representative Plaintiffs and the Nationwide Class if their data had been breached and compromised or stolen.

276. A meeting of the minds occurred, as Representative Plaintiffs and Class Members agreed, *inter alia*, to provide accurate and complete PII/PHI and to pay Defendant in exchange for Defendant's agreement to, *inter alia*, protect their PII/PHI.

277. Representative Plaintiffs and the Nationwide Class Members would not have entrusted their PII/PHI to Defendant in the absence of Defendant's implied promise to adequately safeguard this confidential personal and medical information.

278. Representative Plaintiffs and the Nationwide Class fully performed their obligations under the implied contracts with Defendant.

279. Defendant breached the implied contracts it made with Representative Plaintiffs and the Nationwide Class by making their PII/PHI accessible from the internet (regardless of any mistaken belief that the information was protected) and failing to make reasonable efforts to use the latest security technologies designed to help ensure that the PII/PHI was secure, failing to encrypt Representative Plaintiffs and Class Members' sensitive PII/PHI, failing to safeguard and protect their medical, personal and financial information and by failing to provide timely and accurate notice to them that medical, personal and financial information was compromised as a result of the data breach.

280. Defendant further breached the implied contracts with Representative Plaintiffs and Class Members by failing to comply with its promise to abide by HIPAA and HITECH.

281. Defendant further breached the implied contracts with Representative Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information Defendant created, received, maintained, and

transmitted in violation of 45 CFR 164.306(a)(1).

282. Defendant further breached the implied contracts with Representative Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1).

283. Defendant further breached the implied contracts with Representative Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1).

284. Defendant further breached the implied contracts with Representative Plaintiffs and Class Members by failing 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 CFR 164.308(a)(6)(ii).

285. Defendant further breached the implied contracts with Representative Plaintiffs and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2).

286. Defendant further breached the implied contracts with Representative

Plaintiffs and Class Members by failing 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 CFR 164.306(a)(3).

287. Defendant further breached the implied contracts with Representative Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce violations in violation of 45 CFR 164.306(a)(94).

288. Defendant further breached the implied contracts with Representative Plaintiffs and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq*.

289. Defendant further breached the implied contracts with Representative Plaintiffs and Class Members by failing to design, implement, and enforce policies and procedures establishing physical administrative safeguards to reasonably safeguard protected health information, in compliance with 45 CFR 164.530©.

290. Defendant further breached the implied contracts with Representative Plaintiffs and Class Members by otherwise failing to safeguard Representative Plaintiffs' and Class Members' PII/PHI.

291. Defendant's failures to meet these promises constitute breaches of the

implied contracts.

292. Because Defendant allowed unauthorized access to Representative Plaintiffs' and Class Members' PII/PHI and failed to safeguard the PII/PHI, Defendant breached its contracts with Representative Plaintiffs' and Class Members.

293. Defendant breached its contracts by not meeting the minimum level of protection of Representative Plaintiffs' and Class Members' protected health information and other PII/PHI, because Defendant did not prevent against the breach of over 172,000 patients' PII/PHI.

294. Furthermore, the failure to meet its confidentiality and privacy obligations resulted in Defendant providing goods and services to Representative Plaintiffs and Class Members that were of a diminished value.

295. As a direct and proximate result of Defendant's above-described breach of implied contract, Representative Plaintiffs and Class Members have suffered (and will continue to suffer) (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data; (d) the illegal sale of the compromised data on the dark web; (e) lost work time; and (f) other economic and non-economic harm.

296. As a result of Defendant's breach of implied contract, Representative

Plaintiffs and the Class Members are entitled to and demand actual, consequential, and nominal damages.

FIFTH CLAIM FOR RELIEF
Unjust Enrichment
(On behalf of Representative Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Representative Plaintiffs and the State Subclasses)

297. Representative Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 202.

298. By its wrongful acts and omissions described herein, Defendant has obtained a benefit by unduly taking advantage of Representative Plaintiffs and Class Members.

299. Defendant, prior to and at the time Representative Plaintiffs and Class Members entrusted their PII/PHI and financial information to Defendant for the purpose of obtaining health services, caused Representative Plaintiffs and Class Members to reasonably believe that Defendant would keep such PII/PHI and financial information secure.

300. Defendant was aware, or should have been aware, that reasonable patients and consumers would have wanted their PII/PHI and financial information kept secure and would not have contracted with Defendant, directly or indirectly, had they known that Defendant's information systems were sub-standard for that

purpose.

301. Defendant was also aware that, if the substandard condition of and vulnerabilities in its information systems were disclosed, it would negatively affect Representative Plaintiffs' and Class Members' decisions to seek services therefrom.

302. Defendant failed to disclose facts pertaining to its substandard information systems, defects, and vulnerabilities therein before Representative Plaintiffs and Class Members made their decisions to make purchases, engage in commerce therewith, and seek services or information. Instead, Defendant suppressed and concealed such information. By concealing and suppressing that information, Defendant denied Representative Plaintiffs and Class Members the ability to make a rational and informed purchasing and health care decision and took undue advantage of Representative Plaintiffs and Class Members.

303. Defendant was unjustly enriched at the expense of Representative Plaintiffs and Class Members. Defendant received profits, benefits, and compensation, in part, at the expense of Representative Plaintiffs and Class Members. By contrast, Representative Plaintiffs and Class Members did not receive the benefit of their bargain because they paid for products and/or health care services that did not satisfy the purposes for which they bought/sought them.

304. Since Defendant's profits, benefits, and other compensation were obtained by improper means, Defendant is not legally or equitably entitled to

retain any of the benefits, compensation, or profits it realized from these transactions.

305. Representative Plaintiffs and Class Members seek an Order of this Court requiring Defendant to refund, disgorge, and pay as restitution any profits, benefits, and other compensation obtained by Defendant from its wrongful conduct and/or the establishment of a constructive trust from which Representative Plaintiffs and Class Members may seek restitution.

SIXTH CLAIM FOR RELIEF
Violation of the North Carolina Unfair and Deceptive Trade Practices Act
(N.C. Gen. Stat. § 75-1.1, *et seq.*)
(On behalf of Representative Plaintiff Torres and the North Carolina Subclass)

306. Representative Plaintiff Torres and the North Carolina Subclass re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 202.

307. Representative Plaintiff Torres and the North Carolina Subclass Members further bring this cause of action, seeking equitable and statutory relief to stop the misconduct of Defendant, as complained of herein.

308. Defendant is an entity with subsidiary operations in the state of North Carolina and is subject to the laws and regulations of the State of North Carolina, including but not limited to the North Carolina Unfair and Deceptive Trade Practices Act, N.C. Gen. Stat. § 75.1.1 ("UDTPA"). That act "declare[s] unlawful" all

"[u]nfair methods of competition in or affecting commerce, and unfair of deceptive acts or practices in or affecting commerce." *Id.* § 75-1.1(a).

309. For purposes of North Carolina's UDTPA, the term "commerce" includes all business activities, however denominated, but does not include professional services rendered by a member of a learned profession." *Id.* § 75-1.1(b).

310. Defendant violated the North Carolina UDTPA by engaging in unlawful, unfair, or deceptive business acts and practices in or affecting commerce, as well as unfair, deceptive, untrue, or misleading advertising that constitute acts of "unfair competition" prohibited in the statute.

311. Upon information and belief, the policies, practices, acts and omissions giving rise to this action emanated from Defendant's headquarters and facilities in North Carolina.

312. Defendant engaged in unlawful acts and practices with respect to their services by establishing inadequate security practices and procedures described herein; by soliciting and collecting Representative Plaintiffs Torres' and the North Carolina Subclass Members' sensitive information with knowledge that such information would not be adequately protected; and by gathering Representative Plaintiff Torres' and the North Carolina Subclass Members' sensitive information in an unsecure electronic environment in violation of North Carolina's data breach statute, the Identity Theft Protection Act, N.C. Gen. Stat. § 75-60, *et seq*., which

requires Defendant to undertake reasonable methods of safeguarding the sensitive information of the Representative Plaintiff Torres and the North Carolina Subclass Members.

313. In addition, Defendant engaged in unlawful acts and practices when they failed to discover and then disclose the data security breach to Representative Plaintiff Torres and the North Carolina Subclass Members in a timely and accurate manner, contrary to the duties imposed by N.C. Gen. Stat. § 75-65.

314. Defendant further violated UDTPA by violating North Carolina's Identity Theft Protection Act (ITPA), N.C. Gen. Stat. § 75-60, *et. seq*. ("ITPA") by:

a) Failing to prevent the PII of Representative Plaintiffs Cottam and Torres and the North Carolina Subclass from falling into unauthorized hands;

b) Failing to make reasonable efforts to safeguard and protect the PII/PHI, particularly Social Security numbers, of Representative Plaintiffs Cottam and Torres and the North Carolina Subclass;

c) Failing to provide adequate notice of the security breach to affected patient/consumers upon discovery that their system had been compromised and PII had been disclosed; and

d) In other ways to be discovered and proven at trial.

315. Defendant willfully concealed, suppressed, omitted, and failed to inform Representative Plaintiff Torres and the North Carolina Subclass Members of the material facts as described above.

316. As a direct and proximate result of Defendant's unlawful acts and practices, Representative Plaintiff Torres and the North Carolina Subclass Members

have been injured, suffering ascertainable losses and lost money or property, including but not limited to the loss of their legally protected interests in the confidentiality and privacy of their sensitive information.

317. Defendant knew or should have known that their data security practices were inadequate to safeguard Representative Plaintiffs Torres' and the North Carolina Subclass Members' sensitive information, that the risk of a data security breach was significant, and that their systems were, in fact, breached.

318. Defendant's actions in engaging in the above-named unlawful practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Representative Plaintiff Torres and the North Carolina Subclass Members.

319. Representative Plaintiff Torres and the North Carolina Subclass Members seek relief under the North Carolina UDTPA including, but not limited to: restitution to Plaintiffs Cottam and Torres and the North Carolina Subclass Members of money and property that Defendant have acquired by means of unlawful and unfair business practices; disgorgement of all profits accruing to Defendant because of their unlawful and unfair business practices; treble damages (pursuant to N.C. Gen. Stat. § 75-16); declaratory relief; attorneys' fees and costs (pursuant to N.C. Gen. Stat. § 75-16.1); and injunctive or other equitable relief.

SEVENTH CLAIM FOR RELIEF
Violation of the California Confidentiality of Medical Information Act
(Cal. Civ. Code § 56, *et seq*.)
(On behalf of Representative Plaintiff Juarez and the California Subclass)

320. Representative Plaintiff Juarez and the California Subclass re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 202.

321. 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.

322. 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.

323. 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.

324. 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.

325. Plaintiff Juarez and the California Subclass Members are Defendant's patients, as defined in Civil Code § 56.05(k).

326. Plaintiff Juarez and the California Subclass Members provided their personal medical information to Lincare. At all relevant times, Defendant created, maintained, preserved, stored, abandoned, destroyed, or disposed of medical information in the ordinary course business.

327. As a result of the Data Breach, Defendant has misused, disclosed, and/or allowed third parties to access and view Plaintiff Juarez and the California Subclass 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 medical information was breached as a result of Defendant's negligence.

328. Specifically, Defendant knowingly allowed and affirmatively acted in a manner that actually allowed unauthorized parties to access and view Plaintiff Juarez's and the California Subclass Members' PII/ PHI, 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 Juarez and the California Subclass Members constitutes a violation of Civil Code §§ 56.10, 56.11, 56.13, and 56.26.

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

330. By disclosing Plaintiff Juarez and the California Subclass 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.

331. 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.

332. 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 Juarez's and the California Subclass Members' personal medical information was viewed by, released to, and disclosed to third parties without Plaintiff Juarez's or the California Subclass Members' written authorization.

333. 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 Juarez and the California Subclass 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.

EIGHTH CLAIM FOR RELIEF
Violation of California Consumer Records Act
(Cal. Civ. Code § 1798.82, *et seq*.)
(On behalf of Plaintiff Juarez and the California Subclass)

334. Plaintiff Juarez and the California Subclass re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 202.

335. Section 1798.2 of the California Civil Code requires any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" to "disclose any breach of the security of the system following discovery or notification of the breach in the

security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Under section 1798.82, the disclosure "shall be made in the most expedient time possible and without unreasonable delay . . . ."

336. The CCRA further provides; "Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." (Cal. Civ. Code, § 1798.82(b).)

337. Any person or business that is required to issue a security breach notification under the CCRA shall meet all of the following requirements:

a) The security breach notification shall be written in plain language;

b) The security breach notification shall include, at a minimum, the following information:

1) The name and contact information of the reporting person or business subject to this section;

2) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

3) If the information is possible to determine at the time the notice is

provided, then any of the following:

- The date of the breach;
- The estimated date of the breach; or
- The date range within which the breach occurred. The notification shall also include the date of the notice.

c) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

d) A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and

e) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a Social Security number or a driver's license or California identification card number.

338. The Data Breach described herein constituted a ''breach of the security system" of Defendant.

339. As alleged above, Defendant unreasonably delayed informing Plaintiff Juarez and the California Subclass about the Data Breach, affecting their PII/PHI, after Defendant knew the Data Breach had occurred.

340. Defendant failed to disclose to Plaintiff Juarez and the California Subclass, without unreasonable delay and in the most expedient time possible, the

breach of security of their unencrypted, or not properly and securely encrypted, PII/PHI when Defendant knew or reasonably believed such information had been compromised.

341. Defendant's ongoing business interests gave Defendant incentive to conceal the Data Breach from the public to ensure continued revenue.

342. Upon information and belief, no 1aw enforcement agency instructed Defendant that timely notification to Plaintiff Juarez and the California Subclass would impede its investigation.

343. As a result of Defendant's violation of California Civil Code section 1798.82, Plaintiff Juarez and the California Subclass were deprived of prompt notice of the Data Breach and were thus prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze. These measures could have prevented some of the damages suffered by Plaintiff Juarez and the California Subclass because their stolen information would have had less value to identity thieves.

344. As a result of Defendant's violation of California Civil Code section 1798.82, Plaintiff Juarez and the California Subclass suffered incrementally increased damages separate and distinct from those simply caused by the Data Breach itself.

345. Plaintiff Juarez and the California Subclass seek all remedies available

under California Civil Code section 1798.84, including, but not limited to the damages suffered by Plaintiff Juarez and the California Subclass as alleged above and equitable relief.

346. Defendant's misconduct as alleged herein is fraud under California Civil Code section 3294(c)(3) in that it was deceit or concealment of a material fact known to the Defendant conducted with the intent on the part of Defendant of depriving Plaintiff Juarez and the California Subclass of "legal rights or otherwise causing injury." In addition, Defendant's misconduct as alleged herein is malice or oppression under California Civil Code section 3294(c)(1) and (c) in that it was despicable conduct carried on by Defendant with a willful and conscious disregard of the rights or safety of Plaintiff Juarez and the California Subclass and despicable conduct that has subjected Plaintiff Juarez and the California Subclass to cruel and unjust hardship in conscious disregard of their rights. As a result, Plaintiff Juarez and the California Subclass are entitled to punitive damages against Defendant under California Civil Code section 3294(a).

NINTH CLAIM FOR RELIEF
Violation of California Unfair Competition Law
(Cal. Bus. & Prof. Code, § 17200, *et seq*.)
(On behalf of Plaintiff Juarez and the California Subclass)

347. Plaintiff Juarez and the California Subclass re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 202.

348. Defendant violated California's Unfair Competition Law ("UCL") (Cal. Bus. & Prof. Code, § 17200, et seq.) by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in the UCL, including, but not limited to, the following:

a) by representing and advertising that it would maintain adequate data privacy and security practices and procedures to safeguard their PII and PHI from unauthorized disclosure, release, data breach, and theft; representing and advertising that they did and would comply with the requirement of relevant federal and state laws pertaining to the privacy and security of Plaintiff Juarez's and the California Subclass' PII/PHI; and omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Plaintiff Juarez and the California Subclass' PII/PHI;

b) by soliciting and collecting Plaintiff Juarez's and the California Subclass' PII/PHI with knowledge that the information would not be adequately protected; and by storing Plaintiff Juarez's and the California Subclass' PII/PHI in an unsecure electronic environment;

c) by failing to disclose the Data Breach in a timely and accurate manner, in violation of California Civil Code section 1798.82;

d) by violating the privacy and security requirements of HIPAA, 42 U.S.C. §1302d, *et seq*.;

e) by violating the CMIA, California Civil Code section 56, *et seq*.; and

f) by violating the CCRA, California Civil Code section 1798.82.

349. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff Juarez and the California Subclass. Defendant's practice was also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws like the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1302d, *et seq*., CMIA, Cal. Civ. Code, § 56, et seq., and the CCRA, Cal. Civ. Code, § 1798.81.5.

350. As a direct and proximate result of Defendant's unfair and unlawful practices and acts, Plaintiff Juarez and the California Subclass were injured and lost money or property, including but not limited to the overpayments Defendant received to take reasonable and adequate security measures (but did not), the loss of their legally protected interest in the confidentiality and privacy of their PII/PHI, and additional losses described above.

351. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff Juarez's and the

California Subclass' PII/PHI and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff Juarez and the California Subclass.

352. The California Plaintiffs and the California Subclass seek relief under the UCL, including restitution of money or property that Defendant acquired by means of Defendant's deceptive, unlawful, and unfair business practices, declaratory relief, attorney fees, costs and expenses (pursuant to Cal. Code Civ. Proc., § 1021.5), and injunctive or other equitable relief.

TENTH CLAIM FOR RELIEF
Violation of the Missouri Merchandising Practices Act (Mo. Ann. Stat. § 407.010, *et seq*.)
(On behalf of Representative Plaintiffs B.B. and Chang and the Missouri Subclass)

353. Representative Plaintiffs B.B. and Chang and the Missouri Subclass re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 202.

354. The Missouri Merchandising Practices Act (Mo. Ann. Stat. § 407.010, *et seq*.) (the "MMPA") prohibits the use of any "deception, fraud, false pretense, false promise, misrepresentation, unfair practice or the concealment, suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce".

355. An "unfair practice" is defined by Missouri law, 15 CSR 60-8.020, as any practice which:

a) Either-

1) Offends any public policy as it has been established by the Constitution, statutes or common law of this state, or by the Federal Trade Commission, or its interpretive decisions; or

2) Is unethical, oppressive or unscrupulous; and

b) Presents a risk of, or causes, substantial injury to consumers.

356. Missouri law provides that an "Unfair Practice in General" is "any practice which [o]ffends any public policy as it has been established by the Constitution, statutes or common law of this state, or by the Federal Trade Commission, or its interpretive decisions; or [i]s unethical, oppressive or unscrupulous; and [p]resents a risk of, or causes, substantial injury to consumers." Mo. Code Regs. Ann. tit. 15, § 60-8.020.

357. Missouri law also provides that it "is an unfair practice for any person in connection with the advertisement or sale of merchandise to violate the duty of good faith in solicitation, negotiation and performance, or in any manner fail to act in good faith." Mo. Code Regs. Ann. tit. 15, § 60-8.040.

358. Plaintiff and Defendant are "persons" within the meaning of section 407.010(5).

359. Merchandise is defined by the MMPA, to include the providing of "services" and, therefore, encompasses healthcare services. Healthcare services are a good.

360. Maintenance of the privacy and confidentiality of medical records is a central and not incidental part of the healthcare services Plaintiffs B.B. and Chang and the Missouri Subclass purchased from Defendant. Had Plaintiffs B.B. and Chang and the Missouri Subclass known of Defendant's data security failures, Plaintiffs B.B. and Chang and the Missouri Subclass would not have purchased services from Defendant.

361. Maintenance of medical records are "merchandise" within the meaning of section 407.010(4).

362. The goods and services purchased from Defendant by Plaintiffs B.B. and Chang and the Missouri Subclass were for "personal, family or household purposes" within the meaning of the MMPA.

363. As set forth herein, Defendant's acts, practices and conduct violate the MMPA in that, among other things, Defendant has used and/or continues to use unfair practices, concealment, suppression and/or omission of material facts in connection with the advertising, marketing, and offering for sale of services associated with healthcare services. Such acts offend the public policy established by Missouri statute and constitute an "unfair practice" as that term is used in

Missouri Revised Statute 407.020(1).

364. Defendant's unfair, unlawful and deceptive acts, practices and conduct include: (1) representing to its patients that it will not disclose their sensitive personal health information to an unauthorized third party or parties; (2) failing to implement security measures such as securing the records in a safe place; (3) failing to disclose to its patients, at the time of their relevant purchases, its known security failures; and (4) failing to train personnel.

365. Defendant's conduct also violates the enabling regulations for the MMPA because it: (1) offends public policy; (2) is unethical, oppressive and unscrupulous; (3) causes substantial injury to consumers; (4) it is not in good faith; (5) is unconscionable; and (6) is unlawful.

366. As a direct and proximate cause of Defendant's unfair and deceptive acts, Plaintiffs B.B. and Chang and the Missouri Subclass have suffered damages in that they (1) paid more for medical record privacy protections than they otherwise would have, and (2) paid for medical record privacy protections that they did not receive. In this respect, Plaintiffs B.B. and Chang and the Missouri Subclass have not received the benefit of the bargain and have suffered an ascertainable loss.

367. Plaintiffs B.B. and Chang and the Missouri Subclass seek actual and nominal damages for all monies paid to Defendant in violation of the MMPA. In addition, Plaintiff seeks attorneys' fees.

ELEVENTH CLAIM FOR RELIEF
Violation of New York General Business Law § 349
(On behalf of Representative Plaintiff Miller and the New York Subclass)

368. Representative Plaintiff Miller and the New York Subclass re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 202.

369. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a), including but not limited to the following:

a) Defendant actively and knowingly misrepresented or omitted disclosure of material information to Representative Plaintiff Miller and the New York Subclass at the time they provided such PII and PHI that Defendant did not have sufficient security or mechanisms to protect PII and PHI.

b) Defendant misrepresented material facts to Representative Plaintiff Miller and the New York Subclass by representing that it would maintain adequate data privacy and security practices and procedures to safeguard the PII and/or PHI of Representative Plaintiff Miller and the New York Subclass from unauthorized disclosure, release, data breaches, and theft;

c) Defendant misrepresented material facts to Representative Plaintiff Miller and the New York Subclass by representing that it did and would comply

with the requirements of federal and state laws pertaining to the privacy and security of the PII and PHI of Representative Plaintiff Miller and the New York Subclass;

d) Defendant omitted, suppressed, and concealed material facts of the inadequacy of its privacy and security protections for the PII and PHI of Representative Plaintiff Miller and the New York Subclass;

e) Defendant engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of the PII and PHI of Representative Plaintiff Miller and the New York Subclass, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45); and

f) Defendant engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Data Breach to Representative Plaintiff Miller and the New York Subclass in a timely and accurate manner, contrary to the duties imposed by N.Y. Gen. Bus. Law § 899-aa(2).

370. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the PII and PHI that Representative Plaintiff Miller and the New York Subclass entrusted to Defendant,

and that risk of a data breach or theft was highly likely.

371. Defendant should have disclosed this information because Defendant was in a superior position to know the true facts related to its defective data security.

372. Defendant's failure constitutes false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Representative Plaintiff Miller and the New York Subclass) regarding the security of Defendant's network and aggregation of PII and PHI.

373. The representations upon which consumers (including Representative Plaintiff Miller and the New York Subclass) relied were material representations (e.g., as to Defendant's adequate protection of PII and PHI), and consumers (including Representative Plaintiff Miller and the New York Subclass) relied on those representations to their detriment.

374. Defendant's conduct is unconscionable, deceptive, and unfair, as it is likely to, and did, mislead consumers acting reasonably under the circumstances. As a direct and proximate result of Defendant's conduct, Representative Plaintiff Miller and the New York Subclass have been harmed, in that they were not timely notified of the Data Breach, which resulted in profound vulnerability to their PII and PHI.

375. As a direct and proximate result of Defendant's unconscionable, unfair, and deceptive acts and omissions, the PII and/or PHI of Representative Plaintiff Miller and the New York Subclass was disclosed to third parties without

authorization, which has caused and will continue to cause damage to Representative Plaintiff Miller and the New York Subclass.

376. As a direct and proximate result of Defendant's violations of N.Y. Gen. Bus. Law § 349, Representative Plaintiff Miller and New York Subclass members suffered damages including, but not limited to:

a) Unauthorized use of their PII and/or PHI;

b) Theft of the PII and/or PHI;

c) Costs associated with the detection and prevention of identity theft and unauthorized use of their PII and PHI;

d) Damages arising from the inability to use their PII and/or PHI;

e) Costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address an attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach;

f) The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII and PHI being placed in the hands of criminals; and

g) Damages to and diminution in value of their PII and PHI entrusted to Defendant and the loss of Representative Plaintiff Miller's and New York Subclass Members' privacy.

377. Representative Plaintiff Miller and the New York Subclass seek relief under N.Y. Gen. Bus. Law § 349(h), including, but not limited to, actual damages, treble damages, statutory damages, injunctive relief, and/or attorneys' fees and costs.

RELIEF SOUGHT

WHEREFORE, Representative Plaintiffs, on behalf of themselves and each member of the proposed National Class and the State Subclasses, respectfully request that the Court enter judgment in their favor for the following specific relief against Defendant as follows:

a) That the Court declare, adjudge, and decree that this action is a proper class action and certify each of the proposed classes and/or any other appropriate subclasses under Fed. R. Civ. P. Rule 23 (b)(1), (b)(2), and/or (b)(3), including appointment of Representative Plaintiffs' counsel as Class Counsel;

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

c) That the Court enjoin Defendant, ordering them to cease and desist from unlawful activities in further violation of North Carolina Unfair and Deceptive Trade Practices Act (N.C. Gen. Stat. § 75.1.1, *et seq.*), California Confidentiality of Medical Information Act (Cal. Civ. Code § 56, *et seq.*), California Consumer Records Act (Cal. Civ. Code § 1798.82, *et seq.*),

California Unfair Competition Law (Cal. Bus. & Prof. Code, § 17200, *et seq*.), New York General Business Law § 349, and Missouri Merchandising Practices Act (Mo. Ann. Stat. § 407.010, *et seq*.);

d) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Representative Plaintiffs' and Class Members' PII/PHI, and from refusing to issue prompt, complete, any accurate disclosures to Representative Plaintiffs and Class Members;

e) For injunctive relief requested by Representative Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Representative Plaintiffs and Class Members, including but not limited to an Order:

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

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

iii. requiring Defendant to delete and purge the PII/PHI of Representative Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Representative Plaintiffs and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Representative Plaintiffs' and Class Members' PII/PHI;

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

vi. prohibiting Defendant from maintaining Representative Plaintiffs' and Class Members' PII/PHI on a cloud-based database;

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

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

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

x. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

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

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

f) For prejudgment interest on all amounts awarded, at the prevailing legal rate;

g) For an award of attorneys' fees, costs, and litigation expenses, as allowed by

law; and

h) For all other Orders, findings, and determinations identified and sought in this Complaint.

JURY DEMAND

Representative Plaintiffs, individually and on behalf of the Nationwide Class and/or Subclasses, hereby demands a trial by jury for all issues triable by jury.

Submitted December 30, 2022.

/s/ John A. Yanchunis
John A. Yanchunis
Ryan Maxey
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Tel: (813) 223-5505
jyanchunis@ForThePeople.com
rmaxey@ForThePeople.com

Stephen R. Basser
BARRACK RODOS & BACINE
3300 Two Commerce Square
2001 Market Street
Philadelphia, PA 19103
Tel: 215.963.0660
Fax: 215.963.0838
sbasser@barrack.com

Raina C. Borrelli
TURKE & STRAUSS LLP
613 Williamson St., Suite 201

Madison, WI 53703
Tel: (608) 237-1775
Fax: (608) 509-4423
raina@turkestrauss.com

Alexandra M. Honeycutt
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
800 S. Gay Street, Suite 1100
Knoxville, Tennessee 37929
Tel: (865) 247-0080
ahoneycutt@milberg.com

Carl V. Malmstrom
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC
111 W. Jackson Blvd., Suite 1700
Chicago, Illinois 60604
Tel: (312) 984-0000
Fax: (212) 686-0114
malmstrom@whafh.com