UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF FLORIDA

CHERRY MERRELL, individually and on behalf of all others similarly situated, Plaintiff v. LINCARE HOLDINGS, INC. Defendant.	Civil Action No.: 8:22-cv-2020 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Cherry Merrell ("Plaintiff"), individually and on behalf of herself and all others similarly situated (collectively "Class Members"), by and through her undersigned counsel, brings this class action against Lincare Holdings, Inc. ("Lincare," the "Company," or "Defendant"). Plaintiff alleges as follows upon personal knowledge as to the facts pertaining to herself, and on information and belief as to all other matters.

I. SUMMARY OF THE ACTION

1. Plaintiff brings this class action against Defendant Lincare for damages arising from a cyber-security attack and data breach caused by the Company's failure to adequately safeguard and secure the private, confidential information – personally identifiable information ("PII") and personal health information ("PHI") – of herself and many tens of thousands of other individuals who entrusted such information to Lincare, and which it was required to protect from unauthorized disclosure.

2. The PII and PHI that was exposed to unauthorized hackers included highly sensitive and potentially highly valuable information of the type that is well-known within the broad healthcare industry to be highly valued by hackers who prey upon and use or sell such private information for profit and/or to facilitate fraud and identity theft, as more fully discussed below.

3. Plaintiff is informed and believes that by no later than on or about September 26, 2021, Defendant "discovered that unauthorized third parties gained access to Lincare's database and information system, which included patient files containing PII and/or PHI accessed by cyber-thieves in September 2021 ("Lincare Data Breach" or "Data Breach").[1]

4. Despite discovering the Data Breach on or about September 26, 2021, it was not until over 8 months later, on or about June 6, 2022, that Lincare began providing notice directly to consumers that their PII and PHI had been accessed. This substantial delay in notifying victims of the Lincare Data Breach prevented Plaintiff and similarly situated Class Members from taking affirmative steps to protect their PHI and PII during the over 8-month interval of time. Indeed, Plaintiff and Class Members were wholly unaware of the Data Breach until they received letter(s) from Defendant so informing them.

[1] https://response.idx.us/additional-information/ (last visited September 1, 2022).

5. Plaintiff Merrell received Defendant's notice of the Data Breach event by letter dated on or about June 6, 2022, as more fully noted in Exhibit A attached hereto and made a part hereof.

6. Plaintiff and Class Members entrusted their sensitive confidential information to Defendant – a company engaged in healthcare related sales and activities – which information was compromised and unlawfully accessed due to the Data Breach event. Confidential PII and PHI information, remains in the possession of Defendant, despite the fact that it was accessed by unauthorized third persons, and is currently being maintained without appropriate and necessary safeguards, and oversight, and therefore remains vulnerable to additional hackers and theft.

7. Defendant maintained Class Members' PII and PHI on its computer networks in a condition that was vulnerable to cyber-attacks. The risk of cyber-attack was well-known to Defendant – and to all healthcare related providers and services – and Defendant was continuously on notice at all times material that its failure to take steps necessary to secure the PII and/or PHI from a risk of cyber-attack and unauthorized access left that information and property in a dangerous position that was vulnerable to theft. Defendant was unquestionably aware that data thieves, once armed with PII and/or PHI that they accessed in a data breach, are capable of pursuing numerous types of misconduct and crimes through the unauthorized use and exploitation of that data, including opening new financial accounts in Class Member's names, taking loans in their names, using their names to obtain medical services, obtain government benefits, file fraudulent tax returns in order to get refunds to which they are not even entitled, and numerous other assorted acts of thievery and fraud.

8. This was not the first time Lincare had been cyber-attacked. On February 10, 2017, Lincare notified current and former Lincare employees of a "phishing attack" in which personal file information may have been compromised. This experience placed the Defendant on clear unambiguous notice that it maintained information on its data banks and systems that was highly valuable and sought after by cyber criminals and other unauthorized individuals who could and would attempt to use the information for profit.

9. Nevertheless, and despite this knowledge, Defendant continuously disregarded the rights of Plaintiff and Class Members, as more fully defined below, by, among other things, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its data systems were protected and safeguarded against unauthorized intrusions, while failing to disclose that it did not

have adequately robust computer systems and security safeguards or practices in place with respect to protecting against the risk of unauthorized access of PII and/or PHI. Defendant further failed to take standard and reasonably available steps to prevent the Lincare Data Breach and failed to properly train its staff and employees on proper security measures. Defendant and its employees failed to properly monitor the computer networking systems on which it housed the PII and/or PHI and, had they done so, would have discovered the intrusion sooner, and would not have permitted cyber thieves to freely access Defendant's IT network for a substantial period of time. The Lincare Data Breach was a direct result of Defendant's failures and misconduct.

10. Importantly, Defendant also failed to provide Plaintiff and Class Members with prompt and timely notice of the Lincare Data Breach, thereby further injuring them by such delay.

11. Plaintiff's and Class Members' identities are now at risk as a consequence of Defendant's misconduct. Their PII and/or PHI that was collected by the Defendant and maintained without adequate safeguards at all times material is now in the hands of cyber thieves – a present risk that will continue throughout their respective lifetimes.

12. Plaintiff and Class Members have been exposed to a present and eminent risk of fraud and identity theft and must now and in the future closely monitor their financial accounts to guard against such risk and injury.

13. To that end, Plaintiff and Class Members will necessarily have to incur out-of-pocket costs for purchasing credit monitoring services and taking other protective measures to deter and detect identity theft.

14. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals who are Class Members, and further seeks remedies that include, but are not limited to, compensatory damages, nominal damages and reimbursement of out-of-pocket costs, as well as injunctive and equitable relief to prevent future injury on behalf of herself and the putative class.

15. Plaintiff seeks to hold Defendant responsible for not ensuring that the PHI/PII was maintained in a manner consistent with industry, 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.

II. PARTIES

Plaintiff

16. Plaintiff Cherry Merrell is, and at all times mentioned herein was, a resident of the state of Georgia, residing in Rocky Face, Georgia. Plaintiff purchased and received healthcare related products and related services from Lincare and provided PII and PHI information that was shared with Lincare as a consequence of its services. Plaintiff has been notified by Lincare of the Data Breach and that her PII and/or PHI was compromised, having received a written Notice of Security Incident, Exhibit A hereto, dated June 6, 2022.

Defendant

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

18. 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. Plaintiff 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.

III. JURISDICTION AND VENUE

19. This Court has original jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2), because the matter in controversy, exclusive of interest and costs, exceeds the sum value of $5,000,000.00, consists of putative class membership of greater than 100 members, and is a class action in which some of the members of the Class, are citizens of states different than that of Defendant.

20. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because Defendant is authorized to conduct business within this District, is headquartered in this District, has intentionally availed itself of the laws in this District, and conducts substantial business, including acts underlying the allegations of this complaint, in this District.

IV. FACTUAL ALLEGATIONS

Lincare and its Business

21. 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." Defendant's operation includes dozens of subsidiaries and partners across North America.

22. Plaintiff and Class members paid for and received health-related products or other services from Lincare, and thereby entrusted Lincare with their PII/PHI.

23. Defendant Lincare maintained PHI/PII and financial information respecting which it had a duty to adequately secure from unauthorized disclosure.

24. As a contention of entering into a relationship with Plaintiff and other Class members, Lincare required that they provide to and entrust Defendant with their highly sensitive and confidential PHI/PII and financial information which it, in turn, stored on its system that was ultimately affected by the Data Breach event.

25. In securing such information as a condition of forming a relationship with Plaintiff and Class Members, and storing on its database, Defendant assumed legal and equitable duties. Additionally, it knew and should have known that it was responsible for protecting such private information from unauthorized disclosure.

26. Defendant was aware at all times material of the fact that the healthcare industry and affiliated entities were at risk of experiencing a cyber-security attack and data breach as many have occurred throughout the United States. Given its maintenance of such PII and/or PHI and its knowledge of such risk and its duties, Defendant was responsible for safeguarding the PII and PHI in its possession with respect to each Plaintiff and Class Member.

27. The Data Breach could have been prevented had Defendant properly secured and encrypted and/or more securely encrypted its servers generally, as well as Plaintiff and Class Members private information which it stored. Defendant certainly was on notice of trending data breach attacks over the past several years, which only exacerbates its own negligence in failing to safeguard Plaintiff's and Class Members private information.

28. Further, Defendant knew and should have known of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Breach Notification Rule, 45 CFR §§ 164.400-414, which required Lincare 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." Defendant wholly failed to abide by this requirement, as more fully discussed herein.

29. HIPAA establishes national minimum standards 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 conduct certain health care transactions electronically, and sets minimum standards for Defendant's maintenance of Plaintiff's and Class Members' PHI/PII. More specifically, HIPAA requires appropriate safeguards be maintained by organizations such as Defendant to protect the privacy of personal 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 establishes a series of rights over Plaintiff's and Class Members' PHI/PII, including rights to examine and obtain copies of their health records, and to request corrections thereto.

30. Additionally, the HIPAA Security Rule establishes national standards to protect individuals' electronic personal 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.

The Data Breach Event

31. Sometime in or around and no later than September 2021, unauthorized third parties gained access to Lincare's database and, as a result, sensitive PHI/PII information which included medical information, account and record information, names and dates of birth of members of the class alleged herein.

32. Plaintiff was only informed of this Data Breach event by a letter from the Defendant dated June 6, 2022. It effectively took the Defendant over 8 months since it first discovered the Data Breach event on September 26, 2021, before it began notifying Plaintiff and other members of the class.

33. Lincare did not take necessary and adequate steps to safeguard the PHI/PII which was maintained on its systems and data banks and, was even more egregiously, delayed giving notice to Plaintiff and other Class Members for over 8 months after initially discovering the Data Breach event no later than September 26, 2021.

34. Additionally, the Defendant has still failed to report the total number of affected individuals. Though it has reported to the Massachusetts Attorney General that the Data Breach compromised the PII/PHI of 172,052 individuals, Plaintiff is informed and believes and thereupon alleges that the number of affected individuals is actually higher.

35. Defendant has also reported to Attorney Generals for the states of Montana, New Hampshire, Texas and Washington. And, in that regard, it has disclosed that names, Social Security Numbers, driver's license numbers, and medical health insurance information has been compromised. With regard to residents of the State of Texas, it has disclosed that just in Texas, at least 115,394 Texans have been compromised.

36. The unauthorized third-party hacking or access to Plaintiff's and Class Members' private information and financial information was with the intent of engaging in the misuse of and profiteering from the sale or exploitation of that information. Meanwhile, Lincare continues to have obligations created by HIPAA, state data breach notification laws, industry standards, common law, state statutory law and its own insurances and representations to Plaintiff and Class Members.

37. Defendant's untimely, belated and delayed notice itself created significant harm and heightened risk to Plaintiff and other Class Members. Time is of the essence whenever highly sensitive PHI/PII has been accessed or acquired by cyber criminals or other unauthorized persons or entities. Plaintiff is informed and believes and alleges the acquired data is a consequence of the Data Breach event and has been made available to others on the dark web.

38. As a consequence, Plaintiff and Class Members have been subjected to the present and continuing risk of fraud, identity theft and misuse resulting from the possible publication exfiltration other PHI/PII, and especially in regard to social security numbers and sensitive medical information given that hackers can access and then offer for sale their unencrypted, unredacted private information to criminals.

39. Facing a lifetime of identity theft, and heightened risk of misuse of their proactive misinformation, Defendant has now also burdened Plaintiff and Class Members with having to enroll in inadequate monitoring services in order to protect themselves. But such protection has been severely undermined by Defendant's delay and untimely notice for over 8 months.

40. The cyber-attack occurred as a direct and proximate result of Defendant's failure to prevent the Data Breach and as a consequence of the fact that it did not adhere to commonly accepted securities standards and otherwise failed to detect that its data bases were subject to a security breach.

41. The significant risk of a cyber-attack and data breach was unquestionably foreseeable to Defendant.

Plaintiff's and Class Members' Damages

42. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding PII and PHI and of the foreseeable consequences if its data security, or agent's data security systems were breached, including the significant costs that would be imposed on Plaintiff and the Class as a result of the breach.

43. As a direct and proximate result of Defendant's conduct, Plaintiff and the other Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. They must be vigilant and review their credit reports for suspected incidents of identity theft, and educate themselves about security freezes, fraud alerts, and other steps to protect themselves against identity theft. This ongoing need for monitoring for identity theft and fraud will extend indefinitely into the future.

44. Plaintiff and the other Class Members have suffered and will suffer actual injury due to loss of time and increased risk of identity theft as a direct result of the Data Breach. In addition to any fraudulent charges, loss of use of and access to their account funds, costs associated with their inability to obtain money from their accounts, diminution of value of the data, and damage to their credit, Plaintiff and the other Class Members suffer ascertainable losses in the form of out-of-pocket expenses, opportunity costs, and the time and costs reasonably incurred to remedy or mitigate the effects of the Data Breach.

45. Moreover, Plaintiff and the other Class Members have an interest in ensuring that Defendant implement reasonable security measures and safeguards to maintain the integrity and confidentiality of the PII, and PHI, including making sure that the storage of data or documents containing PII or PHI is not accessible by unauthorized persons and that access to such data is sufficiently protected.

46. In addition to the remedy for economic harm, Plaintiff and the Class Members maintain an undeniable and continuing interest in ensuring that the PII and PHI remains in the possession of Defendant is secure, remains secure, and is not subject to future theft.

Plaintiff's Experiences

47. Beginning in and around February 2013 and through July 2017, Plaintiff received medical care equipment and devices from Lincare that it delivered to her and invoiced her for a portion of the cost. Lincare received Plaintiff's PHI/PII in connection with its services and any follow-on healthcare related services.

48. Plaintiff typically takes measures to protect her PII and PHI and is very careful about sharing her PII and PHI. She has never knowingly transmitted unencrypted PII and PHI over the internet or other unsecured source.

49. Plaintiff Merrell typically stores documents containing her PII and PHI in a safe and secure location. She also diligently chooses unique usernames and passwords for her online accounts.

50. As a result of the Data Breach, Plaintiff Merrell has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. She monitors accounts and credit scores and has sustained emotional distress as a result of worrying about her PII and PHI being exfiltrated. She has monitored her account extensively since receiving the Notice of Data Breach from Defendant and intends to spend time taking steps to protect her PII and PHI. This is time that was and will be lost and unproductive and taken away from other activities and duties.

51. Plaintiff has suffered, and will continue to suffer, lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety, emotional distress, and increased concerns for the loss of her privacy.

52. As a result of the Data Breach and the exfiltration of her unencrypted PII and PHI in the hands of criminals, Plaintiff is at a substantial present risk and will continue to be at an increased risk of identity theft and fraud for years to come.

53. To date, Defendant has done very little to adequately protect Plaintiff and Class Members, other than informing them of the availability of free credit reports and has done nothing to compensate them for their injuries sustained in this Data Breach.

Medical Records Are Uniquely Valuable to Hackers

54. Medical records are uniquely valuable to hackers. Indeed, hackers prey on medical/healthcare entities. And healthcare providers such as Lincare have been aware of this for a number of years and the need to take adequate measures to secure their systems and information. In 2018 alone, over 400 breaches targeting medical data were reported to the Inspector General of the Department of Health and Human Services.[2] That figure represented a substantial increase from the year before. The steady growth of hacks of healthcare entities is no surprise and can be tied to two significant factors, (1) the failure of healthcare entities, like Lincare, to adequately protect patient data and (2) the substantial value of medical records, which include a broad range of PII and PHI. The high value placed on medical records is, according to the head of investigations at the HHS Office of Inspector General, a reflection of the "treasure trove" of data contained within them.[3]

55. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[4] Of the 1,473 recorded data breaches, 525 of them, or 35.64%, were in the medical or healthcare industry.[5] The 525 reported breaches reported in 2019 exposed nearly 40 million sensitive records (39,378,157), compared to only 369 breaches that exposed just over 10 million sensitive records (10,632,600) in 2018. These incidents continue to rise in frequency, with an estimated 1,862 data breaches occurring in 2021.[6]

56. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2022 report, the healthcare compliance company Protenus found that there were 905 medical data

---

[2] https://www.cbsnews.com/news/hackers-steal-medical-records-sell-them-on-dark-web/ and https://www.advisory.com/en/daily-briefing/2019/03/01/hackers (last visited on September 1, 2022).

[3] https://www.cbsnews.com/news/hackers-steal-medical-records-sell-them-on-dark-web/ (last visited on September 1, 2022).

[4] 01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (idtheftcenter.org) (last visited on September 1, 2022).

[5] *Id.*

[6] *Id.*

breaches in 2021 with over 50 million patient records exposed.[7] This is an increase from the 758 medical data breaches which exposed approximately 40 million records that Protenus compiled in 2020.[8] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[9] It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

57. The continued vulnerability of the healthcare industry to hacking is widely recognized within the healthcare industry. An article published on the website of Advisory Board, a company that advises healthcare providers, health insurance companies and others on issues critical to the healthcare industry, recognized that "the cyber threats we face are growing in sophistication and magnitude and becoming more difficult to combat."[10] The article further noted that "[a]s a result, every healthcare organization needs to have a strong strategy in place to mitigate cyber risk."

58. Large healthcare providers like Lincare are well aware of the risk that data breaches pose to consumers, especially because both the size of Lincare's patient base and the fact that the PHI and PII that they collect and maintain from their patients is profoundly valuable to hackers. A 2017 survey by Accenture determined that 50% of healthcare data breach victims eventually suffered medical identity theft, resulting in an average of $2,500 in out of pocket costs per patient.[11] That same survey also highlighted the importance of rapid disclosure of healthcare data breaches as it noted that "half of the survey respondents reported that they learned of the breach themselves – as opposed to an official company

---

[7] PROTENUS, *2022 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/breach-barometer-report (last visited September 1, 2022).

[8] *Id.*

[9] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Date-Use Solutions in 2018, Up 17.5% from 2017,* INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report.

[10] https://www.advisory.com/en/daily-briefing/2019/03/01/hackers, (last visited on September 1, 2022).

[11] Top 10 Biggest Healthcare Data Breaches of All Time | Digital Guardian, (last visited on September 1, 2022).

or law enforcement notification – after they had been alerted to an error on their benefits explanation, credit card statement, or similar documents."[12]

59. Even where hacked healthcare data is not used to steal identities, its theft poses substantial harm to consumers. In February 2021, hackers published "extensive" patient information hacked from two U.S. hospital groups in an extortion effort.[13] The hackers made off with "tens of thousands of files containing patients' personal medical information" from just eleven hospitals.[14] In that breach, detailed medical data was posted, unencrypted, on the dark web including "at least tens of thousands of scanned diagnostic results and letters to insurers. One folder contains background checks on hospital employees. An Excel document titled 2018_colonoscopies has 102 full names, dates and details of the procedures, and a field to mark "yes" or "no" to whether the patient has a 'normal colon.'"[15] Such public posting of confidential PHI and PII is part of a trend to extort money from healthcare providers and/or individual patients, posting detailed medical records and other PII or PHI if victims refuse to pay.

Lincare's Failure to Protect Consumer PHI and PII is a Violation of HIPAA

60. Companies in the Healthcare related business and services such as Lincare are bound by the HIPAA Privacy Rule, 45 CFR §§ 160, 164, which protects all "*individually identifiable health information,*" or PHI "held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral." PHI includes:

> . . . information that is a subset of health information, including demographic information collected from an individual, and:
>
> (1) Is created or received by a healthcare provider, health plan, employer, or health care clearinghouse; and

---

12 *Id.*

13 https://www.nbcnews.com/tech/security/hackers-post-detailed-patient-medical-records-two-hospitals-dark-web-n1256887, last visited on September 1, 2022.

14 https://hacked.com/hackers-medical-records/, last visited on September 1, 2022.

15 Hackers post detailed patient medical records from two hospitals to the dark web (nbcnews.com), last visited on September 1, 2022.

> (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
>
> (i) That identifies the individual; or
>
> (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

45 CFR § 160.103. The privacy rule requires that covered entities, including healthcare providers like Defendant, provide sufficient safeguards to protect the privacy of the PHI entrusted to them by patients. Entities covered by the HIPAA Privacy Rule are required to report breaches of unsecured health information to the Secretary of Housing and Human Services ("HHS") as soon as possible after discovery of the breach. 45 CFR § 164.408. Here, Plaintiff is informed and believes and thereon alleges that if Lincare reported the breach to HHS, it would not have reported the breach to HHS sooner than the same day that Defendant publicly acknowledged the Data Breach, despite acknowledging that they initially discovered the Data Breach over 8 months earlier.

61. HIPAA establishes national minimum standards 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 conduct certain health care transactions electronically, and sets minimum standards for Defendant's maintenance of Plaintiff's and Class Members' PHI/PII. More specifically, HIPAA requires appropriate safeguards be maintained by organizations such as Defendant to protect the privacy of personal 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 establishes a series of rights over Plaintiff's and Class Members' PHI/PII, including rights to examine and obtain copies of their health records, and to request corrections thereto.

62. Additionally, the HIPAA Security Rule establishes national standards to protect individuals' electronic personal 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.

Industry Standards for Data Security

63. In light of the numerous high-profile data breaches targeting companies like Anthem Health Care, Target, Neiman Marcus, eBay, Anthem, Deloitte, T-Mobile, and Equifax, Defendant is, or reasonably should have been, aware of the importance of safeguarding PII and PHI, as well as of the foreseeable consequences of its systems being breached.

64. Security standards commonly accepted among businesses that store PII and PHI using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Monitoring for suspicious or irregular traffic to servers;

c. Monitoring for suspicious credentials used to access servers;

d. Monitoring for suspicious or irregular activity by known users;

e. Monitoring for suspicious or unknown users;

f. Monitoring for suspicious or irregular server requests;

g. Monitoring for server requests for PII and PHI;

h. Monitoring for server requests from VPNs; and

i. Monitoring for server requests from Tor exit nodes.

65. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for cybersecurity and protection of PII and PHI which includes basic security standards applicable to all types of businesses.

66. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an

internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks.

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

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

68. Because Defendant was entrusted with patients and members' PII and PHI, it had, and has, a duty to patients and members to keep their PII and PHI secure.

69. Patients, such as Plaintiff and Class Members, reasonably expect that when their PII and PHI is provided to Defendant, it will safeguard their PII and PHI.

70. Nonetheless, Defendant failed to prevent the Data Breach discussed below. Had Defendant properly maintained and adequately protected its systems, it could have prevented the Data Breach.

V. CLASS ALLEGATIONS

71. Pursuant to Fed. R. Civ. P. 23(b)(1), (b)(2), (b)(3), and (c)(4), Plaintiff asserts common law claims on behalf of herself and all Class Members for negligence, negligence *per se*, breach of implied contract, breach of the implied covenant of good faith and fair dealing, breach of fiduciary duty, breach of duty, and unjust enrichment on behalf of the following Classes (collectively "the Class"), defined as follows:

Nationwide Class: All residents of the United States whose PII or PHI was accessed or otherwise compromised as a result of the Data Breach.

Georgia Class: All residents of the state of Georgia whose PII or PHI was accessed or otherwise compromised as a result of Data Breach.

Members of the Nationwide Class, and the Georgia Class are referred to herein collectively as "Class Members" or "Class."

72. Excluded from the Class are Defendant, any entity in which Defendant has a controlling interest, Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

73. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

74. **Numerosity**: While the exact number of members of the Class is unknown at this time, Plaintiff is informed and believes and thereupon alleges that the number of "persons affected" by the Data Breach is in the tens of thousands making joinder of each individual Class Member impracticable. Ultimately, members of the Class will be easily identified through Defendant' records.

75. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a) Whether Defendant failed to adequately safeguard Plaintiff's and the Class Members' PII and PHI;

b) Whether Defendant failed to protect Plaintiff's and the Class Members' PII and PHI, as promised;

c) Whether Defendant's computer system systems and data security practices used to protect Plaintiff's and the Class Members' PII and PHI violated HIPAA, federal, state, and local laws, or Defendant's duties;

d) Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and the Class Members' PII and PHI properly and/or as promised;

e) Whether Defendant violated the consumer protection statutes, data breach notification statutes, state unfair insurance practice statutes, state insurance privacy statutes, and state medical privacy statutes applicable to Plaintiff and each Class Member;

f) Whether Defendant failed to notify Plaintiff and Class Members about the Data Breach as soon as practical and without delay after the Data Breach was discovered;

g) Whether Defendant acted negligently in failing to safeguard Plaintiff's and the Class Members' PII and PHI;

h) Whether Defendant was contractually bound to protect the confidentiality of Plaintiff's PII and PHI and have reasonable security measures;

i) Whether Defendant's conduct described herein constitutes a breach of its contracts;

j) Whether Plaintiff and the Class Members are entitled to damages as a result of Defendant's wrongful conduct;

k) Whether Plaintiff and the Class Members are entitled to restitution as a result of Defendant's wrongful conduct;

l) What equitable relief is appropriate to redress Defendant's wrongful conduct; and

m) What injunctive relief is appropriate to redress the imminent and currently ongoing

harm faced by Plaintiff and Class Members.

76. **Typicality**: Plaintiff's claims are typical of the claims of the members of the Class. Plaintiff and the Class Members sustained damages as a result of Defendant's uniform wrongful conduct during transactions with them.

77. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of the Class and has retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Class, and there are no defenses unique to Plaintiff. Plaintiff and her counsel are committed to prosecuting this action vigorously on behalf of the members of the proposed Class and have the financial resources to do so. Neither Plaintiff nor her counsel have any interest adverse to those of the other members of the Class.

78. **Risks of Prosecuting Separate Actions**: This case is appropriate for certification because prosecution of separate actions would risk either inconsistent adjudications which would establish incompatible standards of conduct for the Defendant or would be dispositive of the interests of members of the proposed Class. Furthermore, the Lincare database that contained Plaintiff's and Class Members' PII and PHI still exists and is still vulnerable to future attacks – one standard of conduct is needed to ensure the future safety of the Lincare's database.

79. **Policies Generally Applicable to the Class**: This case is appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Plaintiff and proposed Class as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct towards members of the Class and making final injunctive relief appropriate with respect to the proposed Class as a whole. Defendant' practices challenged herein apply to and affect the members of the Class uniformly, and Plaintiff's challenge to those practices hinges on Defendant's conduct with respect to the proposed Class as a whole, not on individual facts or law applicable only to Plaintiff.

80. **Superiority**: This case is also appropriate for certification because class proceedings are superior to all other available means of fair and efficient adjudication of the claims of Plaintiff and the members of the Class. The injuries suffered by each individual member of the Class are relatively small in comparison to the burden and expense of individual prosecution of the litigation necessitated by Defendant's conduct. Absent a class action, it would be virtually impossible for individual members of the

Class to obtain effective relief from Defendant. Even if Class Members could sustain individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties, including the Court, and would require duplicative consideration of the common legal and factual issues presented here. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single Court.

81. **Manageability**: Plaintiff is unaware of any difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

82. The Class may be certified pursuant to Rule 23(b)(2) because Defendant has acted on grounds generally applicable to the Class, thereby making final injunctive relief and corresponding declaratory relief appropriate with respect to the claims raised by the Class.

83. The Class may also be certified pursuant to Rule 23(b)(3) because questions of law and fact common to the Class will predominate over questions affecting individual members, and a class action is superior to other methods for fairly and efficiently adjudicating the controversy and causes of action described in this Complaint.

84. Particular issues under Rule 23(c)(4) are appropriate for certification because such claims present particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein.

VI. CAUSES OF ACTIONS

FIRST CAUSE OF ACTION

Negligence

85. Plaintiff re-alleges and incorporates the allegations of Paragraphs 1-84, above, by reference. Each and every cause of action alleged herein is on behalf of Plaintiff and the Nationwide Class and Georgia Class.

86. Plaintiff and Class Members were required to submit PII and PHI to healthcare providers, including Defendant, in order to obtain insurance coverage and/or to receive healthcare services.

87. Defendant knew, or should have known, of the risks inherent in collecting and storing the PII and PHI of Plaintiff and Class Members.

88. As described above, Lincare owed duties of care to Plaintiff and Class Members whose PII and PHI had been entrusted with Lincare.

89. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII and PHI.

90. Defendant acted with wanton disregard for the security of Plaintiff's and Class Members' PII and PHI. Defendant knew or should have known that Lincare had inadequate computer systems and data security practices to safeguard such information, and Defendant knew or should have known that hackers were lying in wait and/or attempting to access the PII and PHI in healthcare databases, such as Lincare's.

91. A "special relationship" exists between Defendant and the Plaintiff and Class Members. Lincare, entered into a "special relationship" with Plaintiff and Class Members because it collected and/or stored the PII and/or PHI of Plaintiff and the Class Members, which it and stored in its database – information that Plaintiff and the Class Members had been required to provide to Lincare by way of its related healthcare services.

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

93. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known it was failing to meet its duties, and that Defendant's breach would of such duties cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their PII and PHI.

94. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

SECOND CAUSE OF ACTION

Negligence *Per Se*

95. Plaintiff re-alleges and incorporates the allegations of Paragraphs 1-84, above, by reference.

96. Pursuant to the Federal Trade Commission Act (15 U.S.C. §45), Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class

Members' PII and PHI. Plaintiff is a member of the class that is intended to be protected by the Federal Trade Commission Act.

97. Pursuant to HIPAA (42 U.S.C. §1302d et. seq.), Defendant had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' PII and PHI. Plaintiff is a member of the class that is intended to be protected by HIPAA.

98. Defendant breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act (15 U.S.C. § 45) and HIPAA (42 U.S.C. § 1302d *et. seq.*), by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII and PHI.

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

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

101. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their PII and PHI.

102. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

THIRD CAUSE OF ACTION

Breach of Implied Contract

103. Plaintiff re-alleges and incorporates the allegations of Paragraphs 1-84, above, by reference.

104. Plaintiff and Class members entered into an implied contract with Lincare when they obtained or purchased healthcare related services from Lincare's and/or its healthcare providers, and for which they were required to provide their PII and PHI. The PII and PHI provided by Class Members that was collected and stored by Lincare was governed by and subject to privacy duties and policies.

105. Lincare implicitly and/or expressly agreed and was under a duty to safeguard and protect

the PII and PHI of Plaintiff and Class Members and to timely and accurately notify them in the event that their PII or PHI was breached or otherwise compromised.

106. Plaintiff and Class members entered into the implied contracts with the reasonable expectation that Defendant's data security practices and policies were reasonable and consistent with industry standards. Plaintiff and Class members believed that Lincare would use part of the monies paid to Lincare under the implied contracts to fund adequate and reasonable data security practices.

107. Plaintiff and Class members would not have obtained healthcare services from Lincare's affiliated healthcare providers or entrusted their PII and PHI which was provided to and stored by Defendant in the absence of the implied contract or implied terms between them and Lincare and its affiliated healthcare providers. The safeguarding of the PII and PHI of Plaintiff and Class Members and prompt and sufficient notification of a breach was critical to realize the intent of the parties.

108. Plaintiff and Class Members fully performed their obligations under the implied contracts.

109. Lincare breached its implied contracts with Plaintiff and Class members to protect their PII and PHI when it (1) failed to have security protocols and measures in place to protect that information; (2) disclosed that information to unauthorized third parties; and (3) failed to provide timely and accurate notice that their PII and PHI was compromised as a result of the Data Breach.

110. As a direct and proximate result of Lincare's breaches of implied contract, Plaintiff and Class members sustained actual losses and damages as described in detail above and are also entitled to recover nominal damages.

FOURTH CAUSE OF ACTION

Breach of Fiduciary Duty

111. Plaintiff re-allege and incorporate the allegations of Paragraphs 1-84, above, as if fully set forth herein.

112. In light of the special relationship between Defendant and Plaintiff and Class Members, whereby Defendant became guardian of Plaintiff and Class Members' PII and PHI, Defendant became a fiduciary by its undertaking and guardianship of the PII and PHI, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff and Class Members' PII and PHI; (2) to timely notify

Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

113. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of its relationship with its patients, in particular, to keep secure their PII and PHI.

114. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discovery, investigate, and give notice of the Data Breach in a reasonable and practicable period.

115. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' PII and PHI.

116. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

117. Defendant breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' PII and PHI.

118. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their PII and/or PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII and/or PHI; (iv) 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 identity theft; (V) the continued risk to their PII and/or PHI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and/or PHI in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of the services they received.

119. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other

economic and non-economic losses.

FIFTH CAUSE OF ACTION

Unjust Enrichment

120. Plaintiff re-alleges and incorporates the allegations of Paragraphs 1-84, above as if fully set forth herein.

121. Plaintiff brings this claim individually and on behalf of all Class Members.

122. This count is plead in the alternative to the breach of implied contract count, the second count listed in this Complaint.

123. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff and the Class Members.

124. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

125. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and/or its agents and in so doing provided Defendant with their PII and PHI. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their PII and PHI protected with adequate data security.

126. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII and PHI of Plaintiff and Class Members for business purposes.

127. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII and PHI. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

128. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

129. Defendant failed to secure Plaintiff's and Class Members' PII and PHI and, therefore, did not provide full value for the benefit Plaintiff and Class Members provided.

130. Defendant acquired the PII and PHI through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

131. If Plaintiff and Class Members knew that Defendant had not reasonably secured their PII and PHI, they would not have agreed to provide their PII and PHI to Defendant.

132. Plaintiff and Class Members have no adequate remedy at law for some of the harm Defendant caused.

133. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their Private Information is used; (c) the compromise, publication, and/or theft of their PII and/or PHI; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and/or PHI; (e) lost opportunity costs associated with efforts 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 identity theft; (f) the continued risk to their PII and/or PHI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII and PHI in its continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

134. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

135. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them. In the

alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for its services.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Class Members, seeks the following relief:

A. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointed the undersigned as Class counsel, and finding that Plaintiff is the proper representative of the Class requested herein.

B. Plaintiff requests injunctive relief. Awarding injunctive and other equitable relief as is necessary to protect the interests of the Class Members, including:

(i) an order prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

(ii) requiring Defendant to protect all data collected or received through the course of its business in accordance with HIPAA regulations, other federal, state and local laws, and best practices under industry standards;

(iii) requiring Defendant to design, maintain, and test its computer systems to ensure that PII and PHI in its possession is adequately secured and protected;

(iv) requiring Defendant to disclose any future data breaches in a timely and accurate manner;

(v) requiring Defendant to engage third-party security auditors as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis and ordering them to promptly correct any problems or issues detected by these auditors;

(vi) requiring Defendant to audit, test, and train its security personnel to run automated security monitoring, aggregating, filtering and reporting on log information in a unified manner;

(vii) requiring Defendant to implement multi-factor authentication requirements;

(viii) requiring Defendant's employees to change their passwords on a timely and regular basis, consistent with best practices;

(ix) requiring Defendant to encrypt all PII and PHI;

(x) requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

(xi) requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of its network is compromised, hackers cannot gain access to other portions of its systems;

(xii) requiring Defendant to purge, delete, and destroy in a reasonably secure and timely manner PII and PHI no longer necessary for its provision of services;

(xiii) requiring Defendant to conduct regular database scanning and securing checks;

(xiv) requiring Defendant to routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

(xv) requiring Defendant to provide lifetime credit monitoring and identity theft repair services to members of the Class; and

(xvi) requiring Defendant to educate all Class Members about the threats they face as a result of the loss of their PII and PHI to third parties, as well as steps Class Members must take to protect themselves.

C. Plaintiff also requests actual damages, punitive damages, treble damages, statutory damages, exemplary damages, equitable relief, restitution, disgorgement of profits, attorney's fees, statutory costs, and such other and further relief as is just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: September 1, 2022

Respectfully submitted,

GEORGE GESTEN MCDONALD, PLLC

/s/ David J. George
DAVID J. GEORGE
9897 Lake Worth Road, Suite 302
Lake Worth, Florida 33467
Telephone: (561) 232-6002

Florida Bar No. 898579
dgeorge@4-justice.com
eservice@4-justice.com

LORI G. FELDMAN*
102 Half Moon Bay Drive
Croton-on-Hudson, NY 10520
Telephone: (917) 983-9321
NY Bar No. 2389070
lfeldman@4-justice.com
eservice@4-justice.com

BARRACK, RODOS & BACINE
STEPHEN R. BASSER*
SAMUEL M. WARD*
600 West Broadway, Suite 900
San Diego, CA 92101
sbasser@barrack.com
sward@barrack.com
Telephone: (619) 230-0800
Facsimile: (619) 230-1874

EMERSON FIRM, PLLC
JOHN G. EMERSON*
2500 Wilcrest, Suite 300
Houston, TX 77042
jemerson@emersonfirm.com
Telephone: (800) 551-8649
Facsimile: (501) 286-4659

Counsel for Plaintiff Cherry Merrell

**Pro Hac Vice* application to be filed